PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-344349
(43)Date of publication of application : 14.12.2001

(51)Int.Cl. G06F 17/60
G06F 12/14

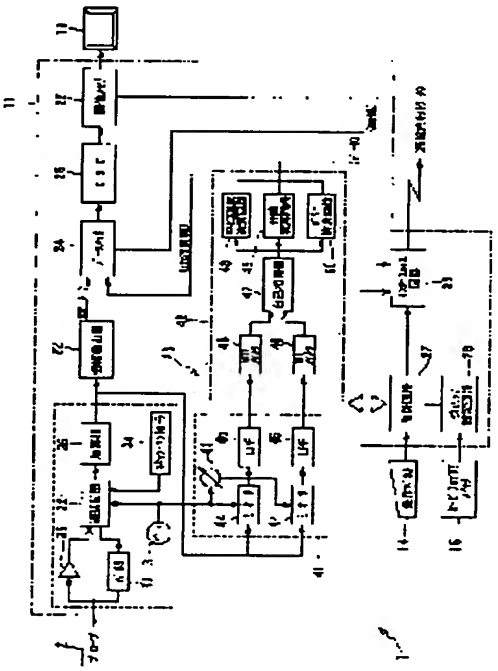
(21)Application number : 2001-075095
(22)Date of filing : 15.03.2001

(71)Applicant : TOSHIBA CORP
(72)Inventor : MIYAJIMA YASUO
SASAKI TAKUYA
HASHIMOTO SHINICHI
KAMIYAMA NAOHISA
YOSHIE TAKESHI
GOTO EIJI
NAKAZATO TOSHIAKI

(30)Priority
Priority number : 2000089707 Priority date : 28.03.2000 Priority country : JP

(54) DIAGNOSTIC IMAGING EQUIPMENT FOR MEDICAL CARE, SECURITY MANAGEMENT METHOD THEREOF AND MAINTENANCE METHOD THEREOF

(57)Abstract:
PROBLEM TO BE SOLVED: To eliminate the possibility of causing malfunctions of specific functions of diagnostic imaging equipment for medical care via a network, and the risk of infringing on patient's privacy, and to allow for enjoying convenience.
SOLUTION: Ultrasonic diagnostic equipment 1 has a service function of being able to be booted up from a service center via a network. This equipment 1 includes, for security management purposes, a security setting circuit 28 and a service permitting switch 5. The security setting circuit 28 has a function that restricts user's access privilege of operating the service function only to a prescribed account, and has a function of authenticating users. The service permitting switch 15 sets user's access privilege to boot up the service function, when the authenticated user's account is other than the account that is restricted by the security setting circuit 28, and has a function that permits or inhibits the access.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－344349
（P2001－344349A）
(43)公開日　平成13年12月14日(2001.12.14)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
Ｇ０６Ｆ	17/60	１２６	Ｇ０６Ｆ 17/60	１２６Ｑ	
		５１２		５１２	
	12/14	３２０	12/14	３２０Ｃ	

審査請求　未請求　請求項の数22　ＯＬ　（全 26 頁）

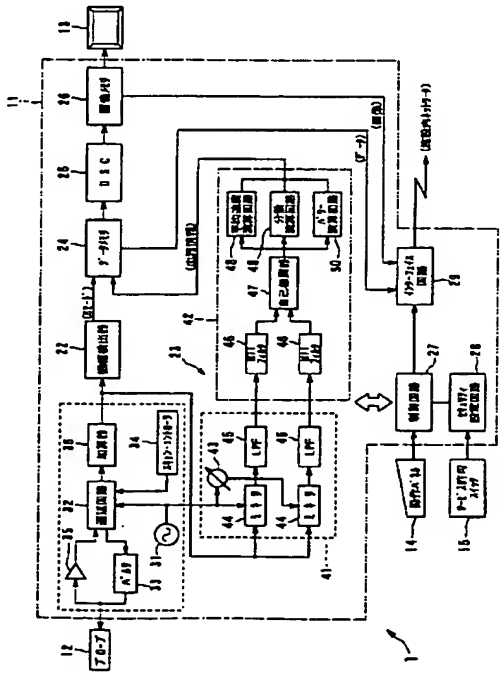
(21)出願番号　特願2001－75095(P2001－75095)
(22)出願日　平成13年３月15日(2001.3.15)
(31)優先権主張番号　特願2000－89707(P2000－89707)
(32)優先日　平成12年３月28日(2000.3.28)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　宮島　泰夫
栃木県大田原市下石上字東山1385番の１
株式会社東芝那須工場内
(72)発明者　佐々木　琢也
栃木県大田原市下石上字東山1385番の１
株式会社東芝那須工場内
(74)代理人　100078765
弁理士　波多野　久　（外１名）

最終頁に続く

(54)【発明の名称】　医療用画像診断装置及びそのセキュリティ管理方法並びにその保守管理方法

(57)【要約】
【課題】医療用画像診断装置の特定機能に対しネットワーク経由で誤動作を生じる可能性や患者のプライバシーを侵害する恐れを解消し、利便性を享受する。
【解決手段】超音波診断装置１は、サービスセンターからネットワーク経由で起動可能なサービス機能を有する。この装置１は、セキュリティ管理上、セキュリティ設定回路２８及びサービス許可スイッチ１５を含む。セキュリティ設定回路２８は、サービス機能を操作するユーザのアクセス権を所定のアカウントのみに制限する機能と、ユーザを認証する機能とを有する。サービス許可スイッチ１５は、認証されたユーザのアカウントがセキュリティ設定回路２８で制限されたアカウント以外の場合にサービス機能の起動に対するユーザのアクセス権を設定し、そのアクセスを許可及び禁止する機能を有する。



【特許請求の範囲】

【請求項１】　遠隔地のコンピュータからネットワークを介して起動可能なサービス機能を有する医療用画像診断装置のセキュリティ管理方法であって、
前記サービス機能を操作するユーザのアクセス権を所定のアカウントのみに制限するステップと、
前記ユーザを認証するステップと、
前記認証されたユーザのアカウントが前記制限されたアカウント以外の場合に前記サービス機能の起動に対する前記ユーザのアクセス権の許可及び禁止を前記医療用画像診断装置側で制御するステップと、を備えたことを特徴とする医療用画像診断装置のセキュリティ管理方法。

【請求項２】　遠隔地のコンピュータにネットワークを介して遠隔診断用の医用画像を供給可能な機能を有する医用画像診断装置のセキュリティ管理方法であって、
前記機能を操作するユーザのアクセス権を所定のアカウントのみに制限するステップと、
前記ユーザを認証するステップと、
前記認証されたユーザのアカウントが前記制限されたアカウント以外の場合に前記機能の起動に対する前記ユーザのアクセス権の許可及び禁止を前記医療用画像診断装置側で制御するステップと、を備えたことを特徴とする医療用画像診断装置のセキュリティ管理方法。

【請求項３】　データベースを成すコンピュータとの間でネットワークを介して患者に関するデータをアクセス可能な機能を有する医用画像診断装置のセキュリティ管理方法であって、
前記機能を操作するユーザのアクセス権を所定のアカウントのみに制限するステップと、
前記ユーザを認証するステップと、
前記認証されたユーザのアカウントが前記制限されたアカウント以外の場合に前記機能の起動に対する前記ユーザのアクセス権の許可及び禁止を前記医療用画像診断装置側で制御するステップと、を備えたことを特徴とする医療用画像診断装置のセキュリティ管理方法。

【請求項４】　遠隔地のコンピュータからネットワークを介して起動可能なサービス機能を有する医療用画像診断装置であって、
前記サービス機能を操作するユーザのアクセス権を所定のアカウントのみに制限するアカウント制限手段と、
前記ユーザを認証する認証手段と、
前記認証手段により認証されたユーザのアカウントが前記アカウント制限手段により制限されたアカウント以外の場合に前記サービス機能の起動に対する前記ユーザのアクセス権の許可及び禁止を制御する制御手段と、を備えたことを特徴とする医療用画像診断装置。

【請求項５】　遠隔地のコンピュータにネットワークを介して遠隔診断用の医用画像を供給可能な機能を有する医療用画像診断装置であって、
前記機能を操作するユーザのアクセス権を所定のアカウントのみに制限するアカウント制限手段と、
前記ユーザを認証する認証手段と、
前記認証手段により認証されたユーザのアカウントが前記アカウント制限手段により制限されたアカウント以外の場合に前記サービス機能の起動に対する前記ユーザのアクセス権の許可及び禁止を制御する制御手段と、を備えたことを特徴とする医療用画像診断装置。

【請求項６】　データベースとの間でネットワークを介して患者に関するデータをアクセス可能な機能を有する医用画像診断装置であって、
前記機能を操作するユーザのアクセス権を所定のアカウントのみに制限するアカント制限手段と、
前記ユーザを認証する認証手段と、
前記認証手段により認証されたユーザのアカウントが前記アカウント制限手段により制限されたアカウント以外の場合に前記サービス機能の起動に対する前記ユーザのアクセス権の許可及び禁止を制御する制御手段と、を備えたことを特徴とする医療用画像診断装置。

【請求項７】　請求項４から６のいずれか１項記載の発明において、前記制御手段は、前記ユーザのアクセス権を自動的に予め定められた手順で設定するスイッチを備えたことを特徴とする医療用画像診断装置。

【請求項８】　請求項４から６のいずれか１項記載の発明において、前記制御手段は、前記ユーザのアクセス権を自動的に予め定められた手順で禁止及び許可するスイッチを備えたことを特徴とする医療用画像診断装置。

【請求項９】　請求項４から６のいずれか１項記載の発明において、前記認証手段は、パスワードでユーザを認証する手段と、前記パスワードを時間的に変化させて前記ユーザに認知させる手段と、を備えたことを特徴とする医療用画像診断装置。

【請求項１０】　請求項９記載の発明において、前記送信手段は、前記パスワードに関するデータを暗号化して送信する手段を備えたことを特徴とする医療用画像診断装置。

【請求項１１】　請求項９記載の発明において、前記送信手段は、前記パスワードに関するデータを複数個に分割して送信する手段を備えたことを特徴とする医療用画像診断装置。

【請求項１２】　請求項４から６のいずれか１項記載の発明において、前記ネットワーク経由の不正アクセスの状況を検出して記録する不正アクセス検出記録手段をさらに備えたことを特徴とする医療用画像診断装置。

【請求項１３】　請求項１２記載の発明において、前記不正アクセス検出記録手段により記録された不正アクセスの回数が規定回数に達したときに前記機能を停止させてその旨を示すメッセージに関するデータを送信する手段をさらに備えたことを特徴とする医療用画像診断装置。

【請求項１４】　請求項９記載の発明において、前記パ

スワードはセキュリティカード方式のものであることを特徴とする医療用画像診断装置。

【請求項１５】　請求項４から６のいずれか１項記載の発明において、前記認証手段は、電子認証を用いてユーザを認証するものであることを特徴とする医療用画像診断装置。

【請求項１６】　請求項４から６のいずれか１項記載の発明において、前記認証手段は、前記ネットワーク経由の通信データの内のＴＣＰ／ＩＰの通信プロトコルに基づくＩＰアドレスを監視してユーザを認証するものであることを特徴とする医療用画像診断装置。

【請求項１７】　請求項４から６のいずれか１項記載の発明において、前記認証手段は、予め登録されたユーザの生理的特徴を利用してユーザを認証するものであることを特徴とする医療用画像診断装置。

【請求項１８】　請求項４から６のいずれか１項記載の発明において、前記制御手段は、前記ユーザの操作が一定時間行われない場合に前記アクセス権を無効又はその起動後の機能に対するアクセス権を解除する手段を備えたことを特徴とする医療用画像診断装置。

【請求項１９】　オペレータの操作により被検者の画像診断が可能な医療用画像診断装置であって、
前記オペレータ固有の操作環境に関するカスタマイズ情報をそのオペレータの識別情報毎に予め登録する情報登録手段と、
前記オペレータをその識別情報で認証する認証手段と、
前記認証手段により認証されたオペレータの識別情報に基づいて前記情報登録手段から前記カスタマイズ情報を検索する情報検索手段と、
前記データ検索手段により検索されたカスタマイズ情報に基づいて前記オペレータ固有の操作環境で操作できるように制御する制御手段と、を備えたことを特徴とする医療用画像診断装置。

【請求項２０】　オペレータの操作により被検者の画像診断が可能な医療用画像診断装置であって、
前記オペレータの操作で使用可能な機能に対して予め設定された複数の使用権限レベルに関する使用権限情報を前記オペレータの識別情報毎に予め登録する情報登録手段と、
前記オペレータをその識別情報で認証する認証手段と、
前記認証手段により認証されたオペレータの識別情報に基づいて前記情報登録手段から前記使用権限情報を検索する情報検索手段と、
前記情報検索手段により検索された使用権限情報に応じた使用権限レベルで前記オペレータの操作で使用可能な機能を制限するように制御手段と、を備えたことを特徴とする医療用画像診断装置。

【請求項２１】　通信回線を介して接続された遠隔地のコンピュータにより保守管理を行うことのできる医療用画像診断装置であって、
前記医療用画像診断装置に設けられ、システム使用者に関する情報を入力するための入力手段と、
前記医療用画像診断装置に設けられ、所定のシステム保守モードへの変更を指示するための操作手段と、
前記操作手段により前記システム保守モードへの変更が指示されたときに前記入力手段により入力された前記システム使用者に関する情報及びその日時情報を前記遠隔地のコンピュータに送信する送信手段と、
前記送信手段により送信された情報に応答して前記遠隔地のコンピュータから前記通信回線経由で送られてくる信号を元に前記医療用画像診断装置のシステム診断、そのシステム設定変更、及びその制御プログラム変更の内の少なくとも１つの作業が可能な状態に切り替える手段とを備えたことを特徴とする医療用画像診断装置。

【請求項２２】　通信回線を介して接続された遠隔地のコンピュータにより医療用画像診断装置を保守管理する方法であって、
前記医療用画像診断装置にシステム使用者に関する情報を入力するステップと、
前記医療用画像診断装置を操作することにより、前記遠隔地のコンピュータから送られてくる信号を元に前記医療用画像診断装置のシステム診断、そのシステム設定変更、及びその制御プログラム変更の内の少なくとも１つの作業が可能なシステム保守モードへの切り替えを指示するステップと、
前記システム保守モードへの切り替えが指示されたときに前記システム使用者に関する情報及びその日時情報を前記通信回線を介して前記遠隔地のコンピュータに送信するステップと、
これで送信された前記システム使用者に関する情報及びその日時情報を前記遠隔地のコンピュータ上の所定の記録媒体上に記憶させる手段とを備えたことを特徴とする医療用画像診断装置の保守管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、超音波診断装置等の医療用画像診断装置及びそのセキュリティ管理方法並びにその保守管理方法に係り、特にネットワークに接続された医療用画像診断装置を利用した不正アクセス等に対するセキュリティ強化・管理技術の工夫に関する。

【０００２】

【従来の技術】超音波診断装置では、近年、汎用コンピュータ技術との融合化が進み、例えばネットワークを介してサービス機能の起動等を制御する遠隔サービスに関する機能や、施設内の患者データにアクセスする機能や、遠隔診断に関する機能等のコンピュータ・ネットワーク関連の機能も装備されつつある。

【０００３】これらの機能を利用すれば、遠隔地からの装置の故障診断、保守、ソフトウェアの版管理等のサービス作業や、遠隔地の医師による遠隔診断、或いは患者

画像データの集中管理なども実現可能となり、これらにより、装置本来の目的である画像診断に対する効率向上に寄与できるものと期待されている。

【０００４】

【発明が解決しようとする課題】しかし、上述した超音波診断装置では、そのサービス機能の利便性とは裏腹に次のような不具合がある。すなわち、この超音波診断装置では、本来、操作者の行使可能な権限の範囲が狭く、セキュリティ管理と言う概念を取り入れておらず、装置の始動に際して操作者を認識する、いわゆる「ログイン」という概念を意識したものではないため、操作者の意図しないデータ等の変更に伴う動作不能や誤動作、或いは悪意の第三者による改ざん等の行為を受けやすい。その結果、装置の動作不良や誤動作が起きたり、患者情報の機密性に対する盲点になりやすかったりする等のセキュリティ上の問題が懸念される。

【０００５】例えば、上記の装置では、操作者の誤動作により超音波診断装置の環境設定ファイルを消去したり又は書き換えてしまったり、装置が再起動不能な状態に陥ったり、明らかに異常であると判別しにくい装置の誤動作に陥ったりする可能性がある。また、この装置では、集中管理されている患者の診断用画像データ、患者名や患者の個人データ、患者の電子カルテ情報が悪意を持って使用されたり、他人が検査者、装置のサービス員、及び医師を装ってデータの不正コピー（盗用）、改ざん、及び消去される恐れもある。

【０００６】上記のようなセキュリティ問題を克服するため、そのセキュリティが必要な機能に対する権限の制限及びその権限所有者への成りすまし防止の仕組みを管理する必要がある。しかし、こういったセキュリティ管理では特に専門知識が必要とされ、その詳細操作を全ての操作者に教育し徹底させることは装置の利便性を損ない、医師等の本来集中すべき診断行為の効率低下や被検者へのサービス低下を伴うと共に、診断行為のコスト上昇につながり、医療システムに経済的悪影響を与えるといった不都合がある。

【０００７】また、近年の超音波診断装置は、使用できる機能が多様化及び複雑化する傾向にあるため、よく使用する機能を容易に使用できるように操作者毎に操作環境をカスタマイズする機能が必須とされている。これに加え、上述のように、近年では、超音波診断装置をネットワークに接続し、このネットワークを介して画像情報や患者情報、その他診断や装置設定に必要な情報を獲得もしくは提供することが多くなってきており、それ以外にも周辺デバイスの充実やその他の理由を背景にして、サービス員ほど設定に熟知していない一般の操作者が高度な装置設定を行う機会が増えている。

【０００８】しかし、上記のような機能の全てを一般の操作者が操作する場合には、次のような問題がある。例えば、他の操作者が設定した操作環境での操作が容易にできるため、その操作環境を使用する以外の操作者によって簡単にその環境を変更することができる。また、機能に対して操作者に与える使用権限は、サービス員用と一般の操作者用の２つのレベルでは不十分で、例えば一般の操作者に対し管理者用と使用者用を分ける等の対応が現状では困難である。従って、最悪の場合、装置の起動に問題を起こすような重要な障害を起こすことも想定される。

【０００９】上記のことは、超音波診断装置以外の医療用画像診断装置の場合も同様に想定される。

【００１０】本発明は、このような従来の問題を考慮に入れてなされたもので、超音波診断装置等の医療用画像診断装置の遠隔診断、患者データ管理、遠隔サービス機能等の特定機能に対する権限限定と成りすまし防止により、装置の誤動作を生じる可能性や患者のプライバシーを侵害する恐れを解消し、これらの機能の利便性を享受することを、その目的とする。

【００１１】特に、本発明は、超音波診断装置等の医療用画像診断装置の遠隔診断や患者データ管理や遠隔サービス等の特定機能に対する権限を個人あるいは団体毎に制限するとともに、操作者あるいは遠隔地よりの接続者について登録されている個人あるいは団体であることを同定する機能を有し、これらの制限の設定が専門の知識がなくても容易に行え、安心してネットワーク等の機能による利便性を活用し、医療コストを低減しつつ被検者に満足度の高い医療行為を提供できる超音波診断装置を提供することを、その目的とする。

【００１２】

【課題を解決するための手段】上記目的を達成するため、本発明に係る医療用画像診断装置及びそのセキュリティ管理方法並びにその保守管理方法は、以下の各側面を有する。

【００１３】第１の側面では、その修理・故障診断・定期点検などに必要な機能、例えば通常の診断とは異なる装置動作の制御、装置内部の状態等の装置への格納、又は得られる情報・データの取得等を有するものである。そして、この装置は、それらの機能を起動させるのに必要なプログラム及びデータのアクセス権が、装置に通常の検査状態でログインするアカウントとは異なる権限のアカウント及び管理者（アドミニストレータ）権限のアカウントのみに制限される。

【００１４】第２の側面では、有線又は無線でネットワークに接続されるものである。この装置は、その修理・故障診断・定期点検などの診断以外の目的で行う機能、例えば有線又は無線で接続されたネットワークを介してアクセスし、装置動作の制御、装置内部の状態等の装置への格納、得られる情報・データの取得等の機能を有するものである。そして、この装置は、これらの機能のアクセス権限を所定の手順で自動的に設定する手段を備える。この手段としては、起動スイッチ手段、ポインタ手

段、音声による起動選択手段等を例示できる。
【００１５】上記の第２の側面では、前記機能をアクセスできるアカウントに対して装置のもつ機能のうち、装置内及び装置が帰属するネットワーク内の病院内情報や患者情報に対してアクセスする機能について、個々に起動許可・不許可の設定を装置内又は装置が帰属するネットワークのみで行う構成が可能である。
【００１６】第３の側面では、ネットワークに接続された超音波診断装置において、診断以外の目的で（装置の修理・故障診断・定期点検などの目的で）ネットワークよりアクセスし、装置の動作を制御、又は／及び、（装置内部の状態等の）装置に格納、又は／及び、得られる情報・データを取得する機能を有し、この機能について、自動的にあらかじめ定められた手順で禁止・許可する（ポインタや音声による起動選択も含めた）スイッチを有するものとする。
【００１７】上記の第２又は第３の側面では、次の構成が可能である。
【００１８】１）装置の帰属するネットワークに接続する際のアカウントのパスワードを装置の起動時に自動的に変更する手段を備える。この場合の変更後のパスワードは、事前に指定された同一又は異なるネットワーク上のメールを含むメッセージとして送信するものとする。この送信は、装置上のファイルでも可能である。
２）不正なパスワード又はアカウントによるアクセスを検出・記録する手段を備える。この場合、アクセス先も記録することが望ましい。
３）パスワードは暗号化される。
４）パスワードに関するデータが複数の分割されて送信される。この場合、不正なアクセスが規定回数に達した場合、機能を停止させると共に、同一又は異なるネットワーク上又は装置上のこれに応じたファイル、或いはメールも含めたメッセージとして送信されることが可能である。
５）パスワードはセキュリティカード方式である。この方式は、例えば経時的にあらかじめ定められた論理で変更される１つ、又は、複数の文字、又は／及び、数字を発行し、装置側にも同一の論理で同一のものを発行するものとする。
６）電子認証を用いたユーザ認識手段を備える。
７）ＴＣＰ／ＩＰのＩＰアドレスを監視するユーザ認識手段を備える。
８）予め登録された個人の生理的特徴を利用するユーザ認識手段を備える。この場合の生理的特徴は、例えば指紋、虹彩のパターン、声紋、顔の特徴等を例示できる。
９）一定時間操作が行われない場合、自動的にアクセス権が無効になるか、或いは起動された機能を解除する手段を備える。
【００１９】第４の側面による超音波診断装置では、装置がサービス機能のためにサービスセンターなどに自発的に通信する際に装置を正しく認識するために時間的に変化するパスワードや電子認証を自動的に行うものとする。
【００２０】第５の側面による超音波診断装置では、オペレータコード及びパスワードの少なくとも一方を用いてオペレータ固有のログインを行い、ログインしたオペレータによるオペレータ固有の設定環境での操作を許容するものとする。
【００２１】第６の側面による超音波診断装置では、オペレータ登録を行い、オペレータによって２つ以上のレベルをつけ、そのレベルによって使える機能に制限をつけるものとする。
【００２２】本発明は、以上の各側面に基づくもので、次のような態様で構成される。
【００２３】請求項１記載の発明は、遠隔地のコンピュータからネットワークを介して起動可能なサービス機能を有する医用画像診断装置のセキュリティ管理方法であって、前記サービス機能を操作するユーザのアクセス権を所定のアカウントのみに制限するステップと、前記ユーザを認証するステップと、前記認証されたユーザのアカウントが前記制限されたアカウント以外の場合に前記サービス機能の起動に対する前記ユーザのアクセス権の許可及び禁止を前記医療用画像診断装置側で制御するステップと、を備えたことを特徴とする。
【００２４】請求項２記載の発明は、遠隔地のコンピュータにネットワークを介して遠隔診断用の医用画像を供給可能な機能を有する医用画像診断装置のセキュリティ管理方法であって、前記機能を操作するユーザのアクセス権を所定のアカウントのみに制限するステップと、前記ユーザを認証するステップと、前記認証されたユーザのアカウントが前記制限されたアカウント以外の場合に前記機能の起動に対する前記ユーザのアクセス権の許可及び禁止を前記医療用画像診断装置側で制御するステップと、を備えたことを特徴とする。
【００２５】請求項３記載の発明は、データベースを成すコンピュータとの間でネットワークを介して患者に関するデータをアクセス可能な機能を有する医用画像診断装置のセキュリティ管理方法であって、前記機能を操作するユーザのアクセス権を所定のアカウントのみに制限するステップと、前記ユーザを認証するステップと、前記認証されたユーザのアカウントが前記制限されたアカウント以外の場合に前記機能の起動に対する前記ユーザのアクセス権の許可及び禁止を前記医療用画像診断装置側で制御するステップと、を備えたことを特徴とする。
【００２６】請求項４記載の発明は、遠隔地のコンピュータからネットワークを介して起動可能なサービス機能を有する医療用画像診断装置であって、前記サービス機能を操作するユーザのアクセス権を所定のアカウントのみに制限するアカウント制限手段と、前記ユーザを認証する認証手段と、前記認証手段により認証されたユーザ

のアカウントが前記アカウント制限手段により制限されたアカウント以外の場合に前記サービス機能の起動に対する前記ユーザのアクセス権の許可及び禁止を制御する制御手段と、を備えたことを特徴とする。

【００２７】請求項５記載の発明は、遠隔地のコンピュータにネットワークを介して遠隔診断用の医用画像を供給可能な機能を有する医療用画像診断装置であって、前記機能を操作するユーザのアクセス権を所定のアカウントのみに制限するアカウント制限手段と、前記ユーザを認証する認証手段と、前記認証手段により認証されたユーザのアカウントが前記アカウント制限手段により制限されたアカウント以外の場合に前記サービス機能の起動に対する前記ユーザのアクセス権の許可及び禁止を制御する制御手段と、を備えたことを特徴とする。

【００２８】請求項６記載の発明は、データベースとの間でネットワークを介して患者に関するデータをアクセス可能な機能を有する医用画像診断装置であって、前記機能を操作するユーザのアクセス権を所定のアカウントのみに制限するアカント制限手段と、前記ユーザを認証する認証手段と、前記認証手段により認証されたユーザのアカウントが前記アカウント制限手段により制限されたアカウント以外の場合に前記サービス機能の起動に対する前記ユーザのアクセス権の許可及び禁止を制御する制御手段と、を備えたことを特徴とする。

【００２９】請求項７記載の発明は、請求項４から６のいずれか１項記載の発明において、前記制御手段は、前記ユーザのアクセス権を自動的に予め定められた手順で設定するスイッチを備えたことを特徴とする。

【００３０】請求項８記載の発明は、請求項４から６のいずれか１項記載の発明において、前記制御手段は、前記ユーザのアクセス権を自動的に予め定められた手順で禁止及び許可するスイッチを備えたことを特徴とする。

【００３１】請求項９記載の発明は、請求項４から６のいずれか１項記載の発明において、前記認証手段は、パスワードでユーザを認証する手段と、前記パスワードを時間的に変化させて前記ユーザに認知させる手段と、を備えたことを特徴とする。

【００３２】請求項１０記載の発明は、請求項９記載の発明において、前記送信手段は、前記パスワードに関するデータを暗号化して送信する手段を備えたことを特徴とする。

【００３３】請求項１１記載の発明は、請求項９記載の発明において、前記送信手段は、前記パスワードに関するデータを複数個に分割して送信する手段を備えたことを特徴とする。

【００３４】請求項１２記載の発明は、請求項４から６のいずれか１項記載の発明において、前記ネットワーク経由の不正アクセスの状況を検出して記録する不正アクセス検出記録手段をさらに備えたことを特徴とする。

【００３５】請求項１３記載の発明は、請求項１２記載の発明において、前記不正アクセス検出記録手段により記録された不正アクセスの回数が規定回数に達したときに前記機能を停止させてその旨を示すメッセージに関するデータを送信する手段をさらに備えたことを特徴とする。

【００３６】請求項１４記載の発明は、請求項９記載の発明において、前記パスワードはセキュリティカード方式のものであることを特徴とする。

【００３７】請求項１５記載の発明は、請求項４から６のいずれか１項記載の発明において、前記認証手段は、電子認証を用いてユーザを認証するものであることを特徴とする。

【００３８】請求項１６記載の発明は、請求項４から６のいずれか１項記載の発明において、前記認証手段は、前記ネットワーク経由の通信データの内のＴＣＰ／ＩＰの通信プロトコルに基づくＩＰアドレスを監視してユーザを認証するものであることを特徴とする。

【００３９】請求項１７記載の発明は、請求項４から６のいずれか１項記載の発明において、前記認証手段は、予め登録されたユーザの生理的特徴を利用してユーザを認証するものであることを特徴とする。

【００４０】請求項１８記載の発明は、請求項４から６のいずれか１項記載の発明において、前記制御手段は、前記ユーザの操作が一定時間行われない場合に前記アクセス権を無効又はその起動後の機能に対するアクセス権を解除する手段を備えたことを特徴とする。

【００４１】請求項１９記載の発明は、オペレータの操作により被検者の画像診断が可能な医療用画像診断装置であって、前記オペレータ固有の操作環境に関するカスタマイズ情報をそのオペレータの識別情報毎に予め登録する情報登録手段と、前記オペレータをその識別情報で認証する認証手段と、前記認証手段により認証されたオペレータの識別情報に基づいて前記情報登録手段から前記カスタマイズ情報を検索する情報検索手段と、前記データ検索手段により検索されたカスタマイズ情報に基づいて前記オペレータ固有の操作環境で操作できるように制御する制御手段と、を備えたことを特徴とする。

【００４２】請求項２０記載の発明は、オペレータの操作により被検者の画像診断が可能な医療用画像診断装置であって、前記オペレータの操作で使用可能な機能に対して予め設定された複数の使用権限レベルに関する使用権限情報を前記オペレータの識別情報毎に予め登録する情報登録手段と、前記オペレータをその識別情報で認証する認証手段と、前記認証手段により認証されたオペレータの識別情報に基づいて前記情報登録手段から前記使用権限情報を検索する情報検索手段と、前記情報検索手段により検索された使用権限情報に応じた使用権限レベルで前記オペレータの操作で使用可能な機能を制限するように制御手段と、を備えたことを特徴とする。

【００４３】請求項２１記載の発明に係る医療用画像診

断装置は、通信回線を介して接続された遠隔地のコンピュータにより保守管理を行うことのできるものであって、前記医療用画像診断装置に設けられ、システム使用者に関する情報を入力するための入力手段と、前記医療用画像診断装置に設けられ、所定のシステム保守モードへの変更を指示するための操作手段と、前記操作手段により前記システム保守モードへの変更が指示されたときに前記入力手段により入力された前記システム使用者に関する情報及びその日時情報を前記遠隔地のコンピュータに送信する送信手段と、前記送信手段により送信された情報に応答して前記遠隔地のコンピュータから前記通信回線経由で送られてくる信号を元に前記医療用画像診断装置のシステム診断、そのシステム設定変更、及びその制御プログラム変更の内の少なくとも１つの作業が可能な状態に切り替える手段とを備えたことを特徴とする。

【００４４】請求項２２記載の発明に係る医療用画像診断装置の保守管理方法は、通信回線を介して接続された遠隔地のコンピュータにより医療用画像診断装置を保守管理する方法であって、前記医療用画像診断装置にシステム使用者に関する情報を入力するステップと、前記医療用画像診断装置を操作することにより、前記遠隔地のコンピュータから送られてくる信号を元に前記医療用画像診断装置のシステム診断、そのシステム設定変更、及びその制御プログラム変更の内の少なくとも１つの作業が可能なシステム保守モードへの切り替えを指示するステップと、前記システム保守モードへの切り替えが指示されたときに前記システム使用者に関する情報及びその日時情報を前記通信回線を介して前記遠隔地のコンピュータに送信するステップと、これで送信された前記システム使用者に関する情報及びその日時情報を前記遠隔地のコンピュータ上の所定の記録媒体上に記憶させる手段とを備えたことを特徴とする。

【００４５】

【発明の実施の形態】以下、本発明に係る医療用画像診断装置及びそのセキュリティ管理方法並びにその保守管理方法の実施の形態を図面を参照して具体的に説明する。以下の例では、医療用画像診断装置に超音波診断装置を例示してあるが、本発明はこれに限らず、Ｘ線診断装置、ＣＴスキャナ、ＭＲＩ、核医学診断装置、内視鏡装置等のモダリティに適用可能である。

【００４６】（第１の実施形態）図１に示す本例の超音波診断装置（医療用画像診断装置）１は、病院等の施設内に構築されたコンピュータ・ネットワーク（以下「施設内ネットワーク」と呼ぶ）１００に接続されている。

【００４７】施設内ネットワーク１００には、本例ではネットワーク管理の制御中枢として機能するサーバ１０１のほか、患者データベース１０２、及びサービス員等が操作する端末（無線端末も含む）１０３が置かれ、これらの各機器１０１～１０３と共に超音波診断装置１がＬＡＮ１０４を介して通信可能に接続されている。

【００４８】この内、サーバ１０１は、所定のネットワークＯＳ（例えば、米国マイクロソフト社のＷｉｎｄｏｗｓＮＴ、ＵＮＩＸ（登録商標）系ＯＳ等）を実装し、そのＯＳ環境でＴＣＰ／ＩＰ等の通信プロトコルをベースにしてネットワーク接続機器（クライアント）からの要求に応じて各種サービスを提供するアルゴリズム（アプリケーション・プログラム）を実行可能なコンピュータ・マシンでなり、本例では例えばＷｉｎｄｏｗｓ ＮＴのＯＳ環境で管理可能なドメイン毎の管理・制御を行う（この機能を有するサーバをＷｉｎｄｏｗｓＮＴでは「ドメインコントローラ」とも言う）。

【００４９】この施設内ネットワーク１００は、専用線、公衆回線等の通信回線２００を介してサービスセンター内に構築されたコンピュータ・ネットワーク（以下「サービスセンター内ネットワーク」と呼ぶ）３００との間で通信可能に接続されている。

【００５０】サービスセンター内ネットワーク３００には、本例ではネットワーク管理の制御中枢として機能するサーバ３０１のほか、サービス員等が操作する端末３０２、及び有線・無線による通信でダイアルアップＩＰ接続が可能なダイアルアップサーバ３０３等が置かれ、これらの各機器３０１～３０３がＬＡＮ３０４を介して通信可能に接続されている。

【００５１】上記のネットワーク接続の構成により、本例の超音波診断装置１では、各種のデータ通信やこれに拠るサービス授受が可能であり、例えば、施設内ネットワーク１００内では患者データベース・システム１０２にアクセスしたり、サービスセンター内ネットワーク３００との間で遠隔サービス作業のための通信を行ったりできる。

【００５２】図２は、本例の超音波診断装置１の構成例を示す。

【００５３】この図２において、超音波診断装置１は、システム全体の制御中枢として機能する装置本体１１と、この装置本体１１に接続される超音波プローブ１２、モニタ１３、操作パネル１４、及びサービス許可スイッチ１５（本発明の制御手段の一部を成す）とを備える。操作パネル１４には、被検体の超音波診断に関する各種条件の設定や変更等のユーザ指示を入力する入力デバイス（スイッチ、キーボード、マウス、トラックボール等）が装備されている。サービス許可スイッチ１５は、サービス作業時に装置１内へのアクセスを許可するもので、例えば、操作パネル１４又はモニタ１３上に予め設定された装置管理用のメニュー中からユーザが選択可能な起動ボタン等で構成される。このスイッチ１５は、これに限らず、ポインタや音声による起動選択等、他の指示手段も採用できる。

【００５４】超音波プローブ１２は、例えばセクタ式電子走査型プローブで構成され、そのプローブ先端部に電

気／機械可逆的変換素子としての圧電セラミック等の複数の圧電振動子がアレイ状に配列されている。これにより、プローブ１２は、装置本体１１から与えられる駆動電圧を超音波パルス信号に変換して被検体内の所望方向に送信する一方、被検体の体内組織の音響インピーダンスの異なる境界で反射され又は微小散乱体により後方散乱された超音波エコー信号をこれに対応する電圧のエコー信号に変換して装置本体１１に送る。このプローブ１２はセクタ式電子走査型プローブに限定されず、リニア式走査型や機械走査型プローブ等でも可能である。

【００５５】装置本体１１は、図２に示すように超音波プローブ１２に接続された送受信回路２１、この送受信回路２１の受信側に置かれた振幅検出器２２、血流情報検出器２３、データメモリ２４、デジタル・スキャン・コンバータ（ＤＳＣ）２５、画像メモリ２６と、操作パネル１４に接続された制御回路（制御部）２７と、サービス許可スイッチ１５に接続されたセキュリティ設定回路（本発明のアカウント制限手段及び認証手段を成す）２８と、施設内ネットワーク１００に接続されたインターフェース回路２９とを備える。

【００５６】上記の装置本体１１の各回路の構成及び動作をさらに説明する。

【００５７】送受信回路２１は、図２に示すように発振器（パルス発生器）３１、遅延回路（送信側及び受信側を含む）３２、パルサ３３、スキャンコントローラ３４、プリアンプ３５、及び加算器３６を備える。

【００５８】発振器３１は、プローブ１２からの超音波ビームの繰り返し周波数を決定するレートパルスを発生し、そのレートパルスを超音波プローブ１２の各振動子数に応じた送信チャンネル数分に分配して遅延回路（送信側）３２に送る。遅延回路３２は、スキャンコントローラ３４から指令されたタイミング信号に応じて遅延時間を可変設定し、その遅延時間をレートパルスに付加して送信チャンネル毎にパルサ３３に供給する。パルサ３３は、レートパルスを受けたタイミングで超音波プローブ１２の各振動子（送信チャンネル）毎に電圧パルスを与える。

【００５９】これにより、送受信回路２１では、プローブ１２の各振動子に与える電圧パルスのタイミングを変えることにより、プローブ１２から被検体内に照射される超音波ビームを電子的に走査したり、フォーカスをかけたりする。スキャンコントローラ３４の制御により遅延回路３２に与える遅延時間を可変することにより、超音波ビームの方向（ラスタ方向）を可変できる。

【００６０】このように送信された超音波ビームは、被検体内の音響インピーダンスの不連続面で反射される。この反射超音波信号は、再びプローブ１２で受信され、対応する電圧量の反射波信号に変換される。この反射波信号はプリアンプ３５で増幅され、遅延回路（受信側）３２により送信時と同一の遅延時間が与えられた後、加算器３６で加算され、振幅検出器２２及び血流情報検出器２３に送られる。

【００６１】振幅検出器２２は、送受信回路２１内の加算器３６からの出力を受けて超音波ビームの各ラスタ方向における反射波の強度を検出し、その検出信号を各ラスタの輝度情報、すなわちＢモード画像（断層像）情報としてデータメモリ２４を介してデジタル・スキャン・コンバータ（ＤＳＣ）２５に送る。

【００６２】血流情報検出器２３は、ドプラシフト検出器４１及びカラードプラ用のＭＴＩ（Ｍｏｖｉｎｇ　Ｔａｒｇｅｔ　Ｉｎｄｉｃａｔｏｒ）演算部４２を備える。

【００６３】ドプラシフト検出器４１は、直交検波方式によりドプラ偏移周波数を検出する回路であり、例えば送受信回路２１内の発振器３１の出力側にその位相を９０度変換する移相器４３と、加算器３６の出力側に２チャンネルに分かれてミキサ４４、４４、及びローパスフィルタ（ＬＰＦ）４５、４５とを備える。各ミキサ４４、４４は、加算器３６の出力と、発振器３１の出力及び位相器４３の出力とをそれぞれ掛け合わせてドプラ偏移周波数と高周波成分（２倍の送信周波数＋ドプラ偏移周波数）を得て、ＬＰＦ４５、４５に送る。ＬＰＦ４５、４５は、ミキサ４３、４３の各出力から高周波成分を除去し、ドプラ偏移周波数の極性も検出可能なコサイン成分及びサイン成分として、ＭＴＩ演算部４２に送る。

【００６４】ＭＴＩ演算部４２は、各ＬＰＦ４５、４５の出力側に順次、Ａ／Ｄ変換器（図示しない）、ＭＴＩフィルタ４６、４６、自己相関器４７、平均速度演算回路４８、分散演算回路（速度分布演算回路）４９、及びパワー演算回路５０を備える。ＭＴＩフィルタ４６、４６は、例えばハイパス特性のデジタルフィルタからなり、各ＬＰＦのＡ／Ｄ変換後の出力に対して固定反射体（血管壁、心壁等）からの不要な反射波（クラッタ成分）を取り除き、自己相関器４７を介して平均速度、分散（速度分布）、パワーの各演算回路４８～５０に供給する。これらの演算回路４８～５０は、平均速度（又は最高速度）、速度分布（又は速度分布値）、血流からの散乱パワー情報を演算し、これらを血流情報としてデータメモリ２４を介してＤＳＣ２５に供給する。

【００６５】ＤＳＣ２５は、振幅検出器２２からのＢモード画像情報と、血流情報検出器２３からの血流情報とを標準テレビジョン方式の画像フォーマットに変換し、これらの画像を画像メモリ２６を介してモニタ１３に出力する。これにより、モニタ１３は、通常の検査状態では画面上に所定フォーマットのＢモード画像や血流情報を表示する。

【００６６】制御回路２７は、例えばＣＰＵ及び記録媒体等を有するマイクロコンピュータを搭載してなり、その記録媒体に予め記録した処理アルゴリズムをＣＰＵで

実行することにより、操作パネル１４からのユーザ指示等に基づいて上述した各回路の動作を制御する。

【００６７】また、この制御回路２７は、上記と同様のマイクロコンピュータの処理により、超音波診断装置１の修理・故障診断・定期点検などの目的で、通常の診断とは異なる装置１の動作・機能、例えばサービス機能や患者情報アクセス機能等を実行し、例えばインターフェース回路２９を介して施設内ネットワーク１００内の各種データ通信やこれに拠るサービス授受を行ったり、サービスセンター内ネットワーク３００との間のサービス処理に関する通信を行ったり、本装置１のネットワーク接続環境・ユーザプロファイル等の設定・変更を行ったりする。

【００６８】セキュリティ設定回路２８は、例えばＣＰＵ及び記録媒体等を有するマイクロコンピュータを搭載してなり、その記録媒体にソフトウェア又はファームウェアとして予め記録した処理アルゴリズムをＣＰＵで実行することにより、サービス許可スイッチ１５の起動に応じて上記の制御回路２７によるサービス機能や患者情報アクセス機能等に対するセキュリティ管理を行う。

【００６９】具体的には、セキュリティ設定回路２８は、本装置１の電源投入時に例えば操作パネル１４（又はモニタ１３等）の所定画面に予め設定されたユーザＩＤやパスワード等の入力を促すログオン（ログイン）画面を表示させ、その入力操作に必要なスイッチ（操作パネル１４上のスイッチ又はサービス許可スイッチ１５）のみを許可し、その他のスイッチや機能等の動作をユーザに応じて制限するようになっている。この場合には、電源投入直後に予め設定されたデフォルトユーザ等のアカウントでログオンしたユーザに対してはサービス機能や患者情報アクセス機能を動作させる権限を制限することも可能である。なお、セキュリティ設定回路２８は制御回路２７と一体に構成することも可能である。

【００７０】ここで、セキュリティ設定回路２８が実行する処理アルゴリズムの内、サービス機能のセキュリティ動作に関する処理例を図１を参照して説明する。

【００７１】図１において、超音波診断装置１にログイン可能な正式のアカウントをもつ操作者としては、超音波診断装置１による通常の検査を行うユーザと、サービス員とを想定する。この場合のサービス員は、サービスセンター内ネットワーク３００の端末３０２を操作するサービス員Ａと、施設内ネットワーク１００の端末１０３を操作するサービス員Ｂとを含む。また、施設内ネットワーク１００のサーバ１０１は、上述したＷｉｎｄｏｗｓＮＴによるドメインコントローラとして、ネットワーク１００内のドメインに参加する超音波診断装置１や端末１０３等の接続機器に対するネットワーク管理を行うものとする。

【００７２】まず、サービス機能のアクセスに際し、悪意を持つ第三者による成りすまし防止のため、セキュリティ設定回路２８では、正しいアカウントをもつ操作者（本例では検査を行うユーザ、サービス員Ａ、Ｂ等）がログオンしたか否かを確認するユーザ認証を行う。このユーザ認証は、本例ではパスワード等に基づくものであるが、これに限らず、例えばユーザの身体情報（指紋、光彩パターン、網膜パターン、顔のプロファイル等）を利用するものでも可能である。

【００７３】上記のユーザ認証の結果、正しいアカウントをもつ操作者がログインした場合には、その操作者に応じた権限を与える。以下、この権限の設定例を説明する。

【００７４】（通常の検査を行うユーザの場合）通常の検査を行うユーザに対しては、操作パネル１４上のサービスを起動させるスイッチの起動を制限し、例えばサービスを行う権限を付与しない。

【００７５】（サービス員の場合）

１）サービス員に対しては、サービス作業を行うために施設内ネットワーク１００の装置１が属するドメインに入って装置１にアクセスする必要があるが、初期状態ではそのドメインに入る権限を付与しない。

【００７６】本例では、例えば、装置側のユーザを通してサービス許可スイッチ１５を起動することでドメイン及び装置１にアクセスすることを許可する方法を採用できる。サービス許可スイッチ１５は、例えば予め設定された装置管理用メニュー中のボタン選択により起動するものである。一例として、例えば定期点検時に装置側のユーザからサービスセンター側のサービス員Ａに調査を依頼後、ユーザの操作で装置１のサービス許可スイッチ１５を起動させるときに設定する。

【００７７】これにより、セキュリティ設定回路２８は、サービス員Ａの端末３０２から施設内ネットワーク１００のドメインへにアクセスを許可するようにドメインに帰属するサーバ１０１に通信し、その後で、サービス員Ａの装置１へのログオンを可能とするように制御する。ここで、サービス員Ａのアカウントは、例えばサービス機能を起動する権限を有するものとする。

【００７８】従って、装置１へのログオン後にサービス員Ａの端末３０２からサービス機能、例えば定期点検に必要な装置自身の動作を確認する自己診断試験を起動させる操作が行われる。その試験結果は、装置内の記録媒体（例えば、セキュリティ設定回路２８のメモリ又はディスク等の記録媒体）内に読み込まれ、インターフェース回路２９を介してネットワーク経由でサービスセンターまで転送され、これにより、装置１の異常有無やその記録が行われる。また、装置１の各ブロックの入力から発生させた時のテストパターンの画像も、同様に装置１からネットワーク経由でサービスセンターまで転送される。さらに、日常のエラーログやイベントログ等についても、同様に装置１内の記録媒体（例えば、セキュリティ設定回路２８内のメモリ又はディスク等の記録媒体）

が読み出され、ネットワーク経由でサービスセンター側に転送される。

【００７９】２）サービス員Ａに対しては、サービスに関する全ての権限を付与することができるが、この場合でも、装置１の帰属するネットワーク１００内にある患者の画像データ、電子カルテ、及び図示しない検査予約システムの情報に対して読み書きする権限を付与せず、これにより、プライバシーの侵害を防止可能とする。

【００８０】３）サービス員Ａは、装置１の動作確認や異常な記録を参照するため、これらの情報をアクセスする必要がある場合は、そのアクセスを許可する権限をもつユーザに装置１に設定された患者データ用のサービス許可スイッチ（アクセス権限許可スイッチ）１５の起動を依頼し、これにより、自身のアクセス権限を有効なものとすることが可能である。この権限は、サービス員Ａがサービス完了報告を発行、すなわち装置１のイベントログにサービス完了を記録するか、ユーザが患者データ用のアクセス権限を初期状態に戻すスイッチを押すと消滅する。

【００８１】４）サービス員に対しては、時間制限でアクセス権限を設定できる。例えば、これらのサービス作業を伴う定期点検を行う日が土曜日に設定されている場合は、それ以前の曜日、例えば金曜日にサービス員Ａに対する権限を土曜日の午前中のみ許可するように事前に権限解除を行うことが可能である。１ヵ月に１回の点検を行う場合も同様である。この場合も権限のあるユーザが点検のための権限解除を事前に行えばよい。このような権限解除に関する動作をユーザ側から行えない場合は、その設定用のプログラムやスクリプト等をサービスセンター側からユーザに送付し、これを開封・実行するだけで事前設定は可能となる。

【００８２】５）サービス員Ａに対しては、複数の権限レベルのアクセス権限を設定できる。例えば、保守管理に関する権限と、内蔵ソフトウェアの版書き換えやシステム領域の情報書き換えの権限とを分け、サービス員の能力・資格に応じて権限を付与する。これは、高度な制御システムの内蔵ソフトウェアの版書き換えやシステム領域の情報書き換えは十分な知識なしに行うと、装置１の動作に大きな問題を与える恐れもあるためである。

【００８３】６）サービス員に対しては、装置１が帰属するネットワーク環境によっては高度のセキュリティが必要な場合もあるため、これに対処するため、時間的にパスワードを暗号化された形で変化させるルールを採用することが可能である。これは、固定したパスワードがネットワーク内を通信され、プライバシー保護が不十分になる場合を回避するものである。

【００８４】この場合の時間的にパスワードを変化させるルールの処理手順は、装置１内の例えばセキュリティ設定回路２８内の記録媒体に予め設定される。サービス員が使用するパスワードを変化させる仕組みは、例えばセキュリティカードによるパスワード発行と同様である。この処理を行えば、仮に第三者によりネットワーク上のアカウント名とパスワードを盗み見られたとしても、それが次々と変化するため、第三者の成りすましをより効果的に防止できる。

【００８５】７）セキュリティ設定回路２８は、誤ったパスワードや未登録のアカウントでアクセスされたことを検出し、規制する機能をもつことが可能である。この機能によれば、不正アクセスが規定回数に達した場合、そのアカウントのログオンを禁止したり、装置１へのログオンをスーパーバイザー等の特定のアカウントを除いて全てのアカウントでのログオンを禁止すると同時に、サービス員又はサービスセンターに不正アクセスの発生を報告する。これにより、外部よりの悪意あるログオンを防止する。

【００８６】８）一方、正規のログオンを行った場合でも、サービス員がログオン中に長時間席を離れる場合等にログオフを失念し、その状態で不正使用されることを防ぐために、サービス権限を持ったログオンをして一定時間（例えば２０分）サービス又は検査の機能や、遠隔又は直接パネルからの操作を行わなかった場合は自動的にログオン時と同じ個人認証を行わないと操作できない状態とする。この状態からは、シャットダウンや再起動は可能とするが、操作の継続はできない。

【００８７】９）サービスセンターからのアクセスであることを確認する手段としては、上記の方法以外に端末のＩＰアドレスを限定したり、電子認証を採用したり、電話回線の電話番号等を限定したりするものが可能である。

【００８８】１０）サービスのためのログオンは、上記のようにネットワーク経由だけでなく、装置１の操作パネル１４から直接行うことも可能である。この場合、装置１は通常、指紋等の個人認証機能を有していないのでパスワードのみ（特に固定のパスワード）サービスで使用できる権限を全て許可しないことが望ましい。装置１の近くにいる場合でも携帯端末を利用して施設内ネットワーク１００から装置１にログオンすることも可能である。

【００８９】１１）電源投入時に装置１内での異常を発見した際に画面で操作者に指示したり、ユーザにメールを送るだけでなく、サービスセンター側にネットワーク接続しその内容・データを報告する場合に自動的にパスワードなどを送信する。この報告の際、上述したように時間的に変化するパスワードを用いるか、或いは電子認証を用いるものが望ましい。

【００９０】この報告の自動応答の結果としてサービスセンター側から応急処置の指示を受ける必要のある異常の場合は、自動的にサービスセンター側からのログオンを可能とする設定を行う。この緊急ログオン用のアカウントは通常のサービスのアカウントとは分けて権限をこ

の機能（応急処置）に限定しセキュリティの低下を防止する。例えば、装置の火災に至る可能性が高い異常などでは、電源停止の応急処置を発行するが、この場合、ユーザがログオン許可をもつことは不合理であり、自動的にサービスセンター側から接続できるようにする。

【００９１】本例では、サービス機能に関する例で説明したが、遠隔診断の目的でドメイン・装置にログオンする際にも同様の方法でセキュリティを確保できる。

【００９２】例えば、図３に示すように装置１の操作者であるユーザ（検査技師）が遠隔地の専門医Ａに特殊な症例の診断を依頼する場合を考える。

【００９３】この場合、専門医Ａの所属する病院等の施設内には、上記サービスセンターの場合と同様にネットワーク（以下「遠隔地ネットワーク」）４００が構築されている。この遠隔地ネットワーク４００には、サーバ４０１、専門医Ａ等が操作する端末４０２、ダイアルアップサーバ４０３等の機器がＬＡＮ４０４を介して通信可能に接続されている。この遠隔地ネットワーク４００は、専用線、公衆回線等の通信回線５００を介して施設内ネットワーク１００に接続されている。

【００９４】まず、この遠隔地の専門医Ａのアカウントに対して装置１内の上述したサービス許可スイッチ１５と同様の役割を担う遠隔診断起動スイッチ１６を起動して接続相手としてこの専門医を選択する。

【００９５】この処理により、専門医Ａは装置１の帰属するドメインに入り、この装置１にログオンすることができる。ログオン後は、画面を自分の端末４０２で見たり、装置１の設定を自分の端末４０２から変更するなどして、患者の診断を行う。患者の過去のデータや別の診断装置のデータ・電子カルテなどの患者情報を装置１の帰属するネットワーク１００上の患者データベース１０２やサーバ１０１などから取得し、これらの情報を参照しながら診断を進めることができる。

【００９６】このとき、全ての患者情報のアクセス権を開放するかどうかは事前あるいは遠隔診断許可時に設定する。遠隔診断が終了すると、必要に応じて医療診療報酬システムに専門医Ａの診療行為に対する処理を行い、患者データをサーバなどに転送し、遠隔診断を終了すると、この専門医Ａのアカウントのドメイン・装置・患者データへのアクセス権は消滅する。継続的に遠隔診断をするためにアクセス権を継続するかの質問を発行して継続使用できるようにしてもよい。

【００９７】従って、本例によれば、超音波診断装置の遠隔診断や患者データ管理や遠隔サービスの機能についての権限を個人あるいは団体毎に制限するとともに、操作者あるいは遠隔地よりの接続者について登録されている個人あるいは団体であることを同定する機能を有し、これらの制限の設定が専門の知識がなくても容易に行え、安心してネットワーク等の機能による利便性を活用し、医療コストを低減しつつ被検者に満足度の高い医療行為を提供できる。

【００９８】次に、実際の運用例を図４～図６に基づいて説明する。この運用例では、超音波診断装置１の属する施設内ネットワーク１００のＬＡＮ１０４の通信プロトコル（ＯＳＩ参照モデル）にＴＣＰ／ＩＰ（トランスポート層／ネットワーク層）及びイーサネット（登録商標）（物理層及びデータリンク層）を適用し、そのＬＡＮ１０４を管理するサーバ１０１のネットワークＯＳに米国マイクロソフト社のＷｉｎｄｏｗｓＮＴを実装した場合を想定している。従って、以下の説明では、ＷｉｎｄｏｗｓＮＴをベースとした呼称として、便宜上、超音波診断装置１の属する施設内ネットワーク１００をネットワークドメイン又は単にドメインと呼ぶ場合があるが、これらは全て同一の概念を表すものとする。

【００９９】最初に、据え付け時の処理例を図４に基づいて説明する。

【０１００】まず、図４に示すように、ステップＳ１にて超音波診断装置１の使用ネットワーク環境を設定する。この場合の設定項目には、例えば装置１の接続されるドメイン名、このドメインにおける装置１のコンピュータ名、ＩＰアドレス、ＷＩＮＳ（Ｗｉｎｄｏｗｓ Ｉｎｔｅｒｎｅｔｗｏｒｋ Ｎａｍｅ Ｓｅｒｖｉｃｅ）、ＤＮＳ（Ｄｏｍａｉｎ Ｎａｍｅ Ｓｙｓｔｅｍ）、及びゲートウェイ等と、装置１の接続されるドメインでのサービス用のリモート用（サービスセンター内からのリモートアクセス用）・オンサイト用（施設内からのアクセス用）でのユーザアカウント名及びその初期パスワードと、等が含まれる。ここで、ＷＩＮＳは、ＷｉｎｄｏｗｓＮＴ環境下のネットワーク管理機能の１つで、ネームサーバ（ホスト名からＩＰアドレスに変換するサーバ）を呼び出すサービスのことを言う。

【０１０１】これらの各設定項目の入力は、例えば所属するサーバ１０１（サイト）のネットワーク管理者等により行われる。その他、装置１の使用ネットワーク環境内にファイヤウォールが構築されている場合、その設定も行う。装置１とサービスセンターとの間のＴＣＰ／ＩＰベースの上位通信プロトコル（セッション層、プレゼンテーション層、アプリケーション層）に本例ではＦＴＰ等を設定する。

【０１０２】次いで、ステップＳ２にてサービスセンターの情報を設定する。この場合の設定項目には、ＦＴＰサイトのＩＰアドレス、その名前、アカウント名、及びパスワードと、サービスセンター内のサービス員における装置１へのユーザ名及びその初期パスワードと、オンサイトのサービス員の装置１へのユーザ名及びそのパスワードと、等が含まれる。

【０１０３】次いで、ステップＳ３にて順次、装置１（サイト）からサービスセンター側への接続試験、サービスセンターから装置１への接続試験、及びサービスセンター側と装置１との相互通信試験を実施する。

【０１０４】次いで、ステップＳ４にて動作確認などの据え付け時サービスをオンサイト（施設側）で実施し、初回サービス結果をサービスセンター側に通信し記録する。また、定期的サービススケジュール及び次回サービススケジュールの各登録を行う。

【０１０５】そして、ステップＳ５にてサービスセンター側へ据え付け時サービス完了を通信し、帰属ネットワークへの次回ログインパスワードを作成し、サーバ（ドメインサーバ）への登録・変更、装置内への記録・変更を行う。また、装置への次回ログインパスワードの作成と装置内への登録・変更、装置内への記録・変更を行う。

【０１０６】以上の据え付け処理が終了すると、実際にサービスセンター側からネットワーク経由で装置１の属するドメインにログオンし装置１のサービス機能に対するリモートアクセスが可能となる。この場合の装置側の処理例及びサービスセンター側の処理例を図５及び図６に示す。

【０１０７】ここで、装置１側のユーザからサービスセンター側にサービス処理を依頼する場合を考える。このサービス処理の開始に際し、図５に示すように、ステップＳ１０にてユーザにより装置１のサービス要求スイッチ（サービス許可スイッチ）１５の起動が行われると、装置１側（制御回路２７）では、ステップＳ１１～Ｓ２５の各処理（図５及び図６）を実行する一方、これに応答してサービスセンター側ではステップＳ３１～Ｓ３９の各処理（図５及び図６）が行われる。

【０１０８】まず、図５に示すように、ステップＳ１１にて上記で設定された正式な権限をもつユーザかどうかがステップＳ１１１～Ｓ１１６の各手順でチェックされる。

【０１０９】すなわち、ステップＳ１１１にてユーザがドメインユーザとして装置１の帰属するネットワーク１００にログオンしているかどうかが判断され、ＹＥＳの場合はステップＳ１２の処理（後述参照）に移行する一方、ＮＯの場合はステップＳ１１２の処理が行われる。このステップＳ１１２においては、ユーザに対してネットワーク１００に接続してログオンすることを促すメッセージを出力される。或いは、自動的にログオンさせるためのナビゲーション機能が起動される。

【０１１０】そして、ステップＳ１１３にてユーザによるログオン処理の中断有無が判断される。この判断でＮＯ（中断する）の場合はステップＳ１１４にて処理終了する一方、ＹＥＳ（中断しない）の場合はステップＳ１１５にてユーザが外部へのデータ送信の権限を有しているかどうかが判断される。この判断でＮＯ（権限無し）の場合は、ユーザに対して外部へのアクセス権限がないので電話でサービスセンターにコールすることを促すメッセージを出す一方、ＹＥＳ（権限有り）の場合は、ステップＳ１２に移行する。

【０１１１】次いで、ステップＳ１２にてサービスセンター側のサーバ３０１に対してＦＴＰによるサービス要求がメッセージ送信され、そのメッセージがサーバ３０１（ＦＴＰサイト）のメッセージボックス内に書き込まれる。このメッセージには、装置１のＩＤ、サイトのＩＤ、及びサービス要求内容を暗号化した情報等が含まれる。

【０１１２】これにより、サービスセンター側では、ステップＳ３１にてＦＴＰサイト内のメッセージボックス内から装置のＩＤ、サイトのＩＤ、サービス要求内容が暗号解読され、これに対応するサービス員が決定され、そのサービス員の情報がＦＴＰのメッセージボックスに書き込まれる。

【０１１３】次いで、装置１側では、ステップＳ１３にてサービスセンター内のサーバからＦＴＰによりサービス員の個人名情報に関するメッセージが取得される。このメッセージには、サービス員のＩＤ、名前の暗号化した情報が含まれる。

【０１１４】次いで、ステップＳ１４にてサービス員の個人名を使用して、帰属するネットワークでのサービス員用のユーザアカウント及びそのログインパスワード、装置１へのログインパスワードが装置１内の記録から読み出され、暗号化される。

【０１１５】次いで、ステップＳ１５にて上記で暗号化されたユーザアカウント及びそのログインパスワード、装置１へのログインパスワードの内の所定の情報を第１のメッセージとしてＦＴＰを利用してサービスセンター内のメッセージボックスに書き込まれる。そして、ステップＳ１６にて上記の暗号化した残りの情報を第２のメッセージとしてＦＴＰを利用してサービスセンター内のメッセージボックスに書き込まれる。

【０１１６】これにより、サービスセンター側では、上記のステップＳ１５及びＳ１６による第１及び第２のメッセージを受けると、ステップＳ３２にて、ＦＴＰサイト内のメッセージボックス内から装置の帰属するネットワークのドメインでのサービス員のユーザアカウント、サービス員のユーザアカウント、ログインパスワード、装置１へのログインパスワードが解読される。

【０１１７】そして、サービスセンター側では、ステップＳ３３にて、装置１の帰属するネットワークドメインにログインし、さらに装置１内の共有ファイルエリアにあるメッセージボックスにサービスに使用するコマンドメッセージを書き込む処理が行われる。

【０１１８】これと並行して、装置１側では、ステップＳ１７にて、サービスセンター側のステップＳ３３の処理によりＦＴＰ内のメッセージボックスへのコマンドメッセージが書き込まれるのを待ち、一定時間メッセージが来ない場合にアボート処理が行われる。そして、サービスセンター側のステップＳ３３の処理によりＦＴＰ内のメッセージボックスにコマンドメッセージが書き込ま

れると、ステップＳ１８にて、そのコマンドメッセージが解読され、そのコマンドメッセージにより指示されたサービス処理が開始される。これと同時に、コマンドメッセージを受け付けた旨のメッセージがサービスセンター側に送信される。

【０１１９】この間、サービスセンター側では、ステップＳ３４及びＳ３５にて、装置１側からコマンド受け付けを示すメッセージを待ち、そのメッセージが一定時間来ない場合にアボート処理が行われる。

【０１２０】その後、装置１側では、ステップＳ１９にて、上記のサービス処理が完了すると、その結果を含めて処理完了を示すメッセージが送信される。

【０１２１】すると、サービスセンター側では、ステップＳ３６にて、装置１側のステップＳ１９の処理により受信したサービス処理の完了結果に基づいて次回に必要な処理が決定される。そして、ステップ３７にて、全てのサービス処理が完了したかどうかが判断される。この判断でＮＯ（完了せず）の場合、上記ステップＳ３３～Ｓ３７の各処理が繰り返される一方、ＹＥＳ（完了）の場合、ステップＳ３８にて今回のサービス報告書が作成され、次回サービス予定が更新され、その次回サービス予定が装置１に送信される。

【０１２２】そして、装置１側では、ステップＳ２０にて、サービスセンター側から指示された処理が次回サービス予定の変更か、それとも終了処理かどうかが判断される。この判断でＮＯの場合、上記ステップＳ１７～Ｓ２０の各処理が繰り返される一方、ＹＥＳの場合、ステップＳ２１にて次回サービス予定が更新される。

【０１２３】また、サービスセンター側では、ステップＳ３９にて、終了指示が装置１に送信され、その後で、装置１からの受け付けが確認される。

【０１２４】これと並行して、装置１側では、ステップＳ２２にて、サービスセンター側からの終了処理の指示を待ち、その指示を受けると、その受け付けた旨がサービスセンター側に返信される。

【０１２５】次いで、ステップＳ２３にてサービス員用のリモートサービス用のネットワークドメインへのログインパスワード、担当したサービス員用の装置へのログインパスワードが変更される。そして、ステップＳ２４にて、担当したサービス員用の装置へのログインパスワード、ネットワークドメインでのログインパスワードが変更して記録される。その後、ステップＳ２５にて、サービス処理完了が表示され、ログアウト確認メッセージ後に、装置１及びそのネットワークドメインからのログアウトが行われる。

【０１２６】（第２の実施形態）図７に示す超音波診断装置１は、上記と同様の構成のほか、セキュリティ設定回路２８（又は制御回路２７）の制御の元で動作し、装置１内又は装置１が通信可能に接続されるネットワーク（上述した施設内ネットワーク１００等）上に配置されるデータベース３０を有する。

【０１２７】データベース３０は、オペレータ（ユーザ）毎にその属性として「使用権限」の情報及びそのオペレータ固有の操作環境の「カスタマイズ情報」を予めデータ登録し管理する。この内、「使用権限」の情報は、例えばユーザに応じて２以上のレベル、例えばオペレータレベル、管理者レベル、サービス員レベル等が設定される。本例では、３つのレベル（ｌｅｖｅｌ）１～３、即ち使用権限の低いものから順にレベル１：通常の検査に関する操作を行う医者や検者、レベル２：装置１の属するネットワーク環境のＩＰアドレス等の設定や変更を行うネットワーク管理者、レベル３：装置１の故障診断等を行うサービス員を例示する。また、「カスタマイズ情報」は、ユーザインターフェース（ＧＵＩ等）、初期値情報、システムプリセット等の操作環境に関する情報を含むもので、本例ではユーザ毎にカスタム（参照用インデックス）の１～４として設定される。

【０１２８】ここで、データベース３０を制御するセキュリティ設定回路２８の処理例を図７に基づいて説明する。

【０１２９】まず、ステップＳ５０にて、装置ログイン時にユーザインターフェースとなるモニタ１３上にオペレータコード及びそのパスワードの少なくとも一方の入力を促す画面（ログイン画面）が表示される。

【０１３０】そして、ステップＳ５１にて、オペレータによりオペレータコード等の入力が行われると、その入力を元にステップＳ５２にてユーザの認証が行われる。このユーザ認証において、ユーザが非登録者の場合、以後の操作を行うことができないか、或いはデフォルトユーザとして使用権限の一番低いレベルでログインさせる。

【０１３１】上記のステップＳ５２の処理によりユーザが登録者の場合、ステップＳ５３にてデータベース３０で検索・照合され、データベース３０に登録されたそのオペレータ固有の操作環境に関するカスタマイズ情報と機能に対する使用権限の情報が得られる。そこで、ステップＳ５４にて、これらのカスタマイズ情報と使用権限の情報に応じたＧＵＩの表示がモニタ１３上で行われ、これにより、オペレータに応じた操作環境が構築される。以後、例えば、権限の許された機能に関係する入力スイッチのみが表示される。或いは、その機能に割り当てられたハードスイッチのみ使用可能となる。

【０１３２】ここで、従来の超音波診断装置の場合でも、オペレータ毎にユーザの好みの操作環境やサービス員用の機能を提供・用意するものが知られているが、これらの機能は、いずれもあるメニュー等からオペレータが操作環境を選択したり、あるパスワードを入力したりするもので、いわばそのオペレータでない人間であってもその機能を使う、または使える可能性があり、装置のセキュリティ上問題が残るものである。

【０１３３】これと比べ、本例によれば、特にオペレータ毎に好みの操作環境を提供する場合又は特に装置のセキュリティ等に関する機能に対して、例えばオペレータが誰なのか、例えばサービス員か、管理者か、通常のオペレータかによって、即ちオペレータのレベルに応じて使用できる機能に制限を設け、装置起動時、ログオン時、オペレータ変更時にユーザ名とパスワードを要求し、あらかじめ装置に登録したユーザに対して与えられた使用権限から、権限のある機能のみを使用できるようにしたため、ユーザレベルによる機能利用権限を分け、従来例と比べると装置のセキュリティをより一層確保することができる。

【０１３４】なお、使用権限については管理者などのオペレータが適宜作成することも可能である。この場合には、新しい権限レベルを作成し、そのレベルに対して意図する機能の使用権限を与える手法等を採用することができる。また、オペレータを登録する際には新規権限レベルを割り当てることができる。

【０１３５】本発明は、その趣旨の範囲内で、上記に限らず、種々の変形実施が可能である。

【０１３６】（第３の実施形態）図８～図１０は、本発明の第３の実施形態に係る医療用画像診断装置（超音波診断装置）及びその保守管理方法を説明するものである。

【０１３７】図８及び図９に示すコンピュータネットワークは、前述した施設内ネットワーク１００内の患者データベース・システム１０２の代りにダイアルアップサーバ（又はモデム）１０５を設け、超音波診断装置１のサービス許可スイッチ１５の代りにシステム保守モードへの切り替えを指示するための操作手段を成すシステム保守モード用スイッチ１５ａを設けたもので、その他の構成は前述した図１及び図３の場合と基本的に同様である。

【０１３８】図１０は、本例の動作例を説明するものである。図１０において、超音波診断装置１は、その起動等のログイン時に際し、前述した図７に示す場合と同様に、セキュリティ回路２８の処理により、システム使用者に対しオペレータコード及びパスワードの入力を促すログイン画面を表示し（ステップＳ５０）、このログイン画面上でシステム使用者によりそのオペレータコード及びパスワードが入力されると（ステップＳ５２）、そのオペレータコード及びパスワードを元にシステム使用者を認証し（ステップＳ５３）、その認証後にデータベース３０上のデータを検索してシステム使用者に対応する使用権限、操作環境のカスタマイズ情報を獲得し（ステップＳ５３）、その使用権原に応じたＧＵＩ（グラフィカル・ユーザ・インターフェース）を表示することでシステム使用者毎に設定された操作環境を構築する（ステップＳ５４）。

【０１３９】そして、超音波診断装置１の保守管理に際し、システム使用者によるシステム保守モード用スイッチ１５ａの操作によりシステム保守モードへの切り替えの指示があるか否かを判断し（ステップＳ５５）、この判断でＹＥＳ（システム保守モードへの切り替え指示あり）の場合のみ、システム使用者に関する情報及びその日時情報をセンター側のサーバ３０１（図８）又は４０１（図９）に送信し（ステップＳ５６）、これに応答してセンター側のサーバ３０１又は４０１から送られてくる所定の保守管理承認用の制御信号を元に、超音波診断装置１のシステム診断、そのシステム設定変更、及びその制御プログラム変更の内の少なくとも１つの作業が可能な状態に切り替える（ステップＳ５７、Ｓ５８）。

【０１４０】これによれば、遠隔地のコンピュータによりメンテナンスを行うことのできる超音波診断装置において、そのシステム診断、そのシステム設定の変更、装置内の制御プログラム等のソフトウェアのアップグレード（変更）等のサービス・メンテナンス作業時間を短縮でき、その作業による超音波診断装置のダウンタイムを短縮できる。また、ネットワーク経由でのデータ送信が可能になるため、ソフトウェアのアップグレード等で最新バージョンのリリース時間も短縮できる。さらに、最新バージョンのソフトウェアについて一元管理ができるため、アップグレード作業における誤りがなくなる。また、装置の故障情報やシステム診断情報のデータ収集効率も向上するようになる。また、一元管理ができるため、保守、開発に対するフィードバックが早くなり、サービス全体の信頼性も向上するようになる。さらに、システム使用者の保守承認記録を残すことも可能となる。

【０１４１】

【発明の効果】以上説明したように、本発明によれば、サービス機能や患者情報へのアクセス機能の権限設定と成りすまし防止により、装置の誤動作を生じる可能性や患者のプライバシーを侵害する恐れもなく、これらの機能の利便性を享受できる。

【０１４２】すなわち、超音波診断装置等の医療用画像診断装置の遠隔診断や患者データ管理や遠隔サービスの機能についての権限を個人あるいは団体毎に制限するとともに、操作者あるいは遠隔地よりの接続者について登録されている個人あるいは団体であることを同定する機能を有し、これらの制限の設定が専門の知識がなくても容易に行え、安心してネットワーク等の機能による利便性を活用し、医療コストを低減しつつ被検者に満足度の高い医療行為を提供できる。

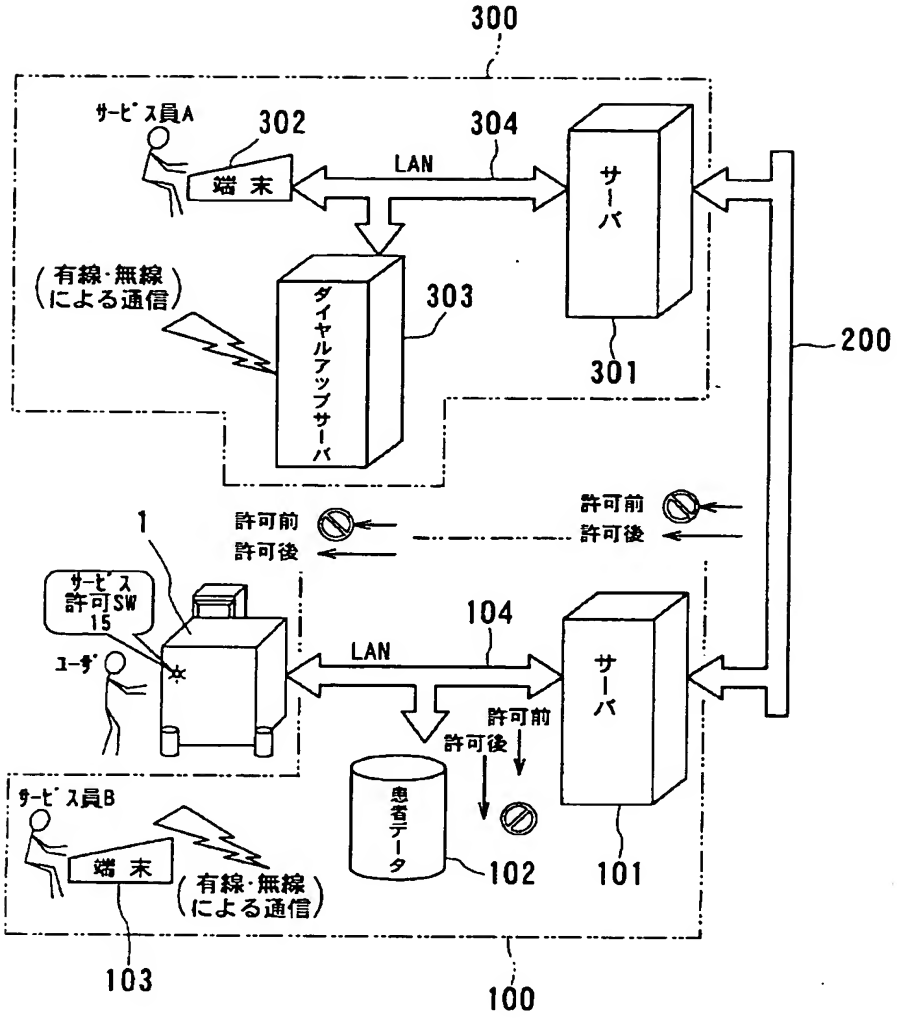
【０１４３】また、本発明の別の側面では、オペレータ固有の操作環境を作成でき、他のオペレータが設定した操作環境を変更してしまう可能性がなくなり、機能に対し、２つ以上の使用権限を与えることで、多様化した機能の使用権限を明確にできる。

【図面の簡単な説明】

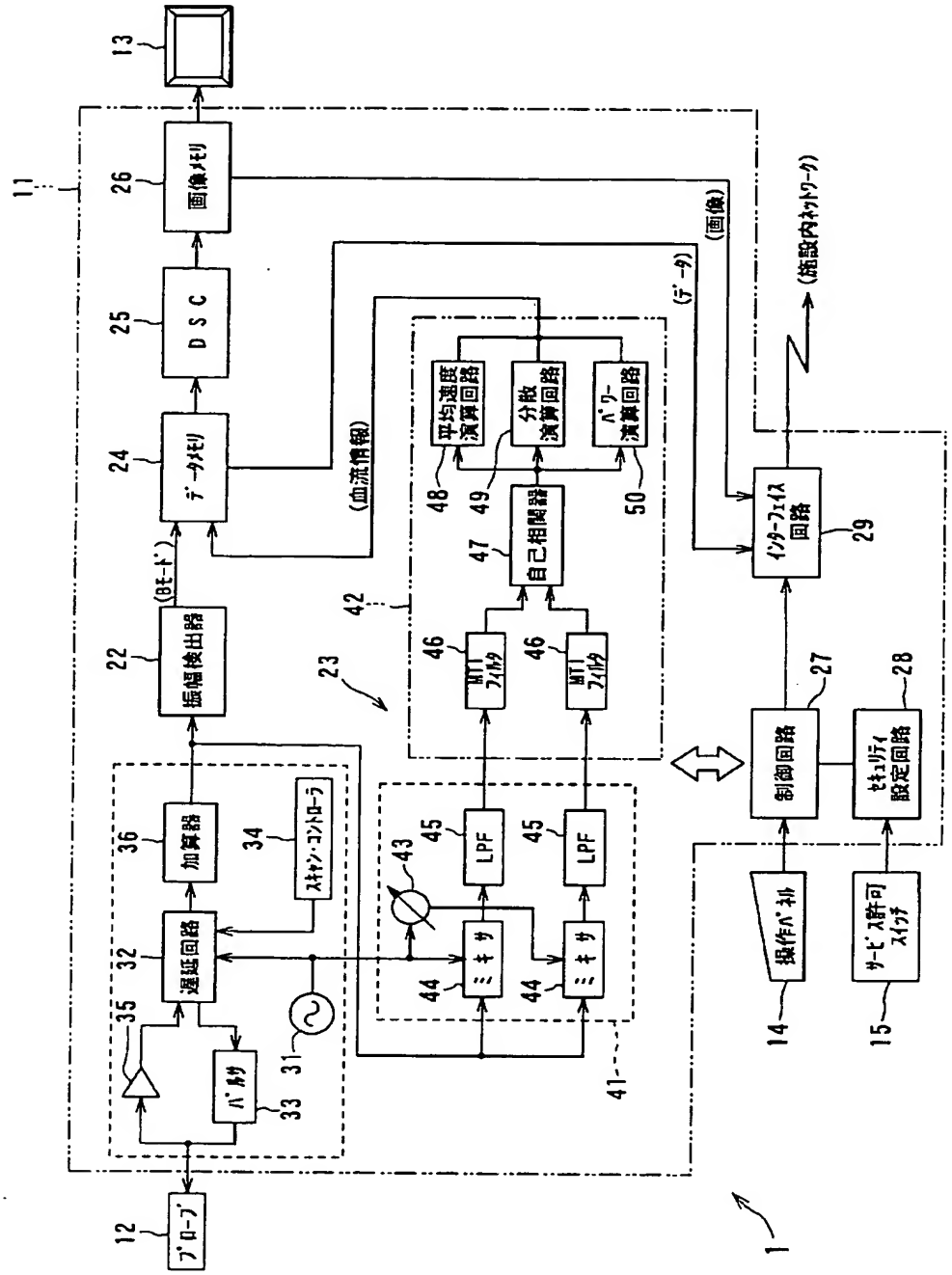
【図１】本発明の第１の実施形態に係る医療用画像診断

装置及びそのセキュリティ管理方法を示す全体構成図。
【図２】第１の実施形態に係る超音波診断装置の全体構成を示す概略ブロック図。
【図３】遠隔診断の場合に適用した例を説明する概要図。
【図４】運用例の据え付け処理を説明する概略フローチャート。
【図５】運用例の装置側及びサービスセンター側の各処理を示す概略フローチャート。
【図６】図５に続く各処理を示す概略フローチャート。
【図７】本発明の第２の実施形態に係る医療用画像診断装置及びそのセキュリティ管理方法を説明する全体構成図。
【図８】本発明の第３の実施形態に係る医療用画像診断装置及びその保守管理方法を説明する全体構成図。
【図９】第３の実施形態において遠隔診断の場合に適用した例を説明する概要図。
【図１０】保守管理時の動作例を説明する図。
【符号の説明】
１　超音波診断装置
１１　装置本体
１２　超音波プローブ
１３　モニタ
１４　操作パネル
１５　サービス許可スイッチ
１６　遠隔診断許可スイッチ
２１　送受信回路
２２　振幅検出器
２４　血流情報検出器
２５　デジタル・スキャン・コンバータ（ＤＳＣ）
２６　画像メモリ
２７　制御回路
２８　セキュリティ設定回路
２９　インターフェース回路
３１　発振器
３２　遅延回路
３３　パルサ
３４　スキャンコントローラ
３５　プリアンプ
３６　加算器
４１　ドプラ検出器
４２　ＭＴＩ演算部
４３　移相器
４４、４４　ミキサ
４５、４５　ローパスフィルタ（ＬＰＦ）
４６、４６　ＭＴＩフィルタ
４７　自己相関器
４８　平均速度演算回路
４９　分散演算回路
５０　パワー演算回路
１００　施設内ネットワーク
１０１　サーバ
１０２　患者データベース・システム
１０３　端末
１０４　ＬＡＮ
２００　通信回線
３００　サービスセンター内ネットワーク
３０１　サーバ
３０２　端末
３０３　ダイアルアップサーバ
３０４　ＬＡＮ
４００　遠隔地ネットワーク
４０１　サーバ
４０２　端末
４０３　ダイアルアップサーバ

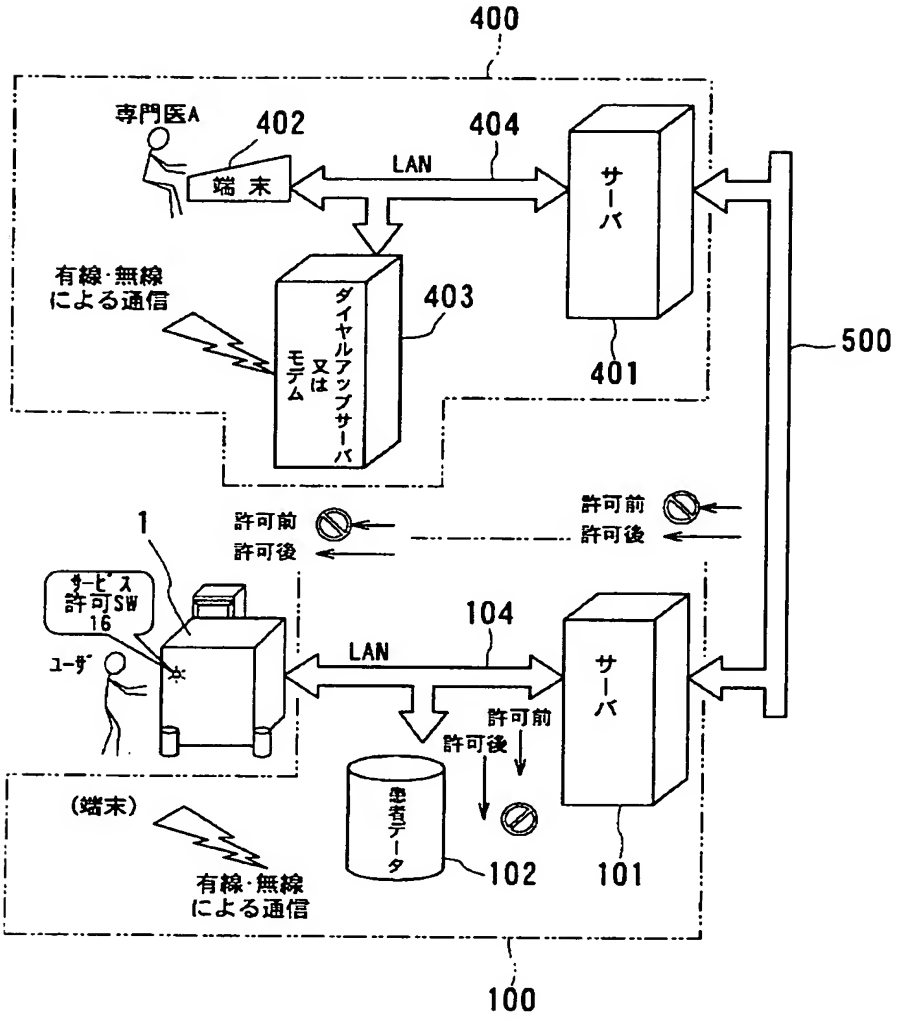
【図１】


300
ｻｰﾋﾞｽ員A
302
端 末
304
LAN
サーバ
(有線・無線による通信)
303
ダイヤルアップサーバ
301
200
許可前
許可後
許可前
許可後
1
サービス許可SW 15
ユーザ
104
LAN
サーバ
許可前
許可後
患者データ
102
101
ｻｰﾋﾞｽ員B
端 末
(有線・無線による通信)
103
100

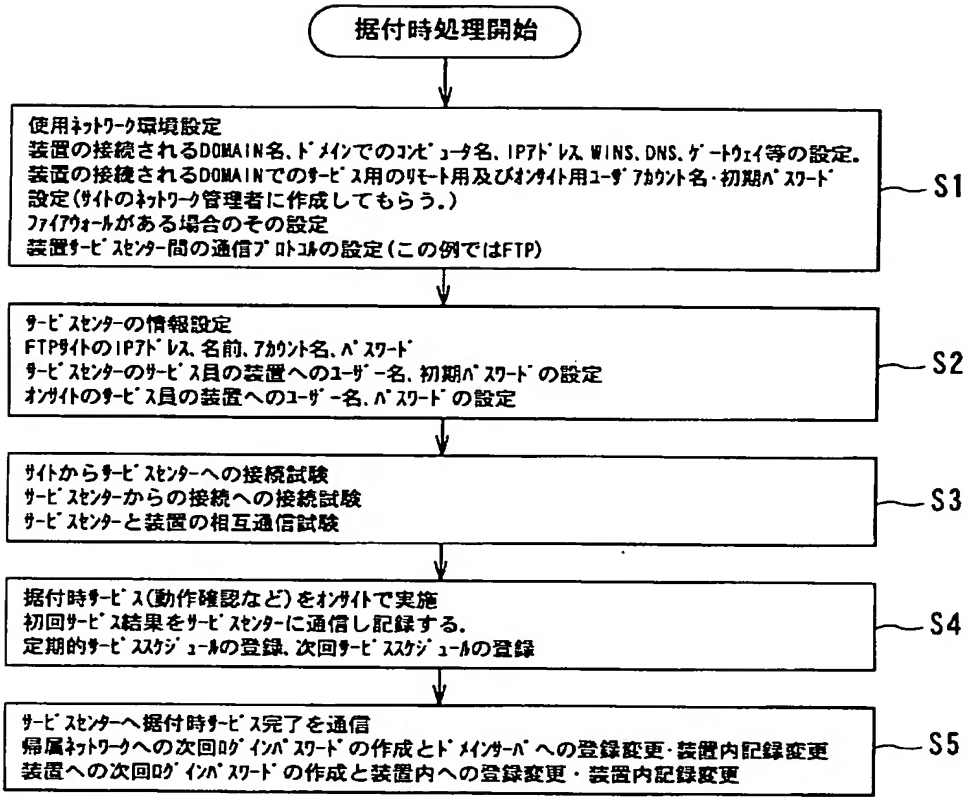
【図２】


13
11
26
画像メモリ
25
DSC
24
データメモリ
(Bモード)
22
振幅検出器
(血流情報)
(画像)
(データ)
(施設内ネットワーク)
平均速度演算回路
分散演算回路
パワー演算回路
48
49
50
47
自己相関器
42
23
46
MTIフィルタ
46
MTIフィルタ
インターフェイス回路
29
43
45
LPF
45
LPF
44
ミキサ
44
ミキサ
制御回路
27
セキュリティ設定回路
28
36
加算器
34
スキャン・コントローラ
32
遅延回路
35
31
33
パルサ
41
操作パネル
14
サービス許可スイッチ
15
12
プローブ
1

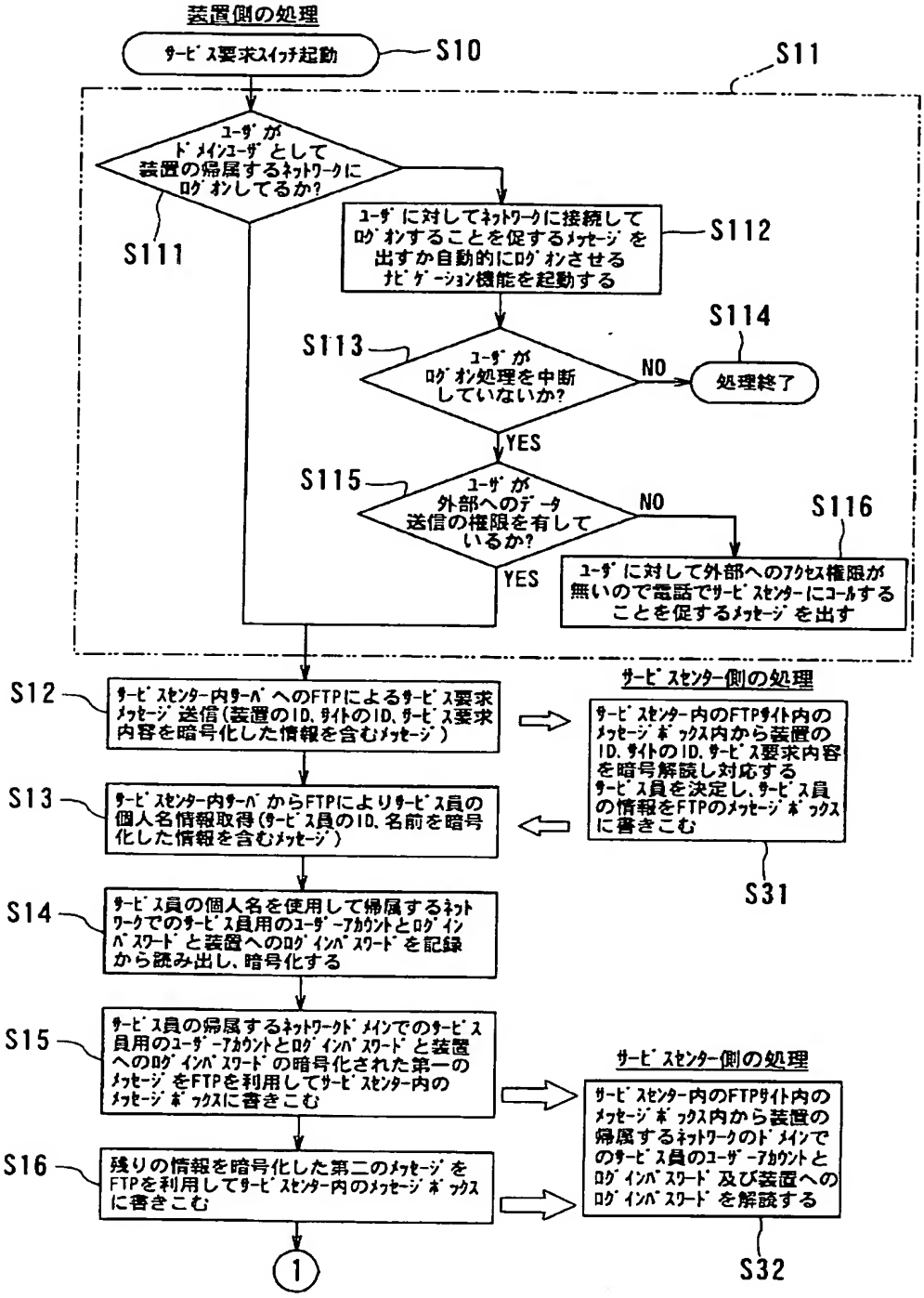
【図３】


400
専門医A
402
端末
LAN
404
サーバ
有線・無線
による通信
ダイヤルアップサーバ
又は
モデム
403
401
500
許可前
許可後
許可前
許可後
1
サービス
許可SW
16
ユーザ
104
LAN
サーバ
許可前
許可後
患者データ
(端末)
有線・無線
による通信
102
101
100

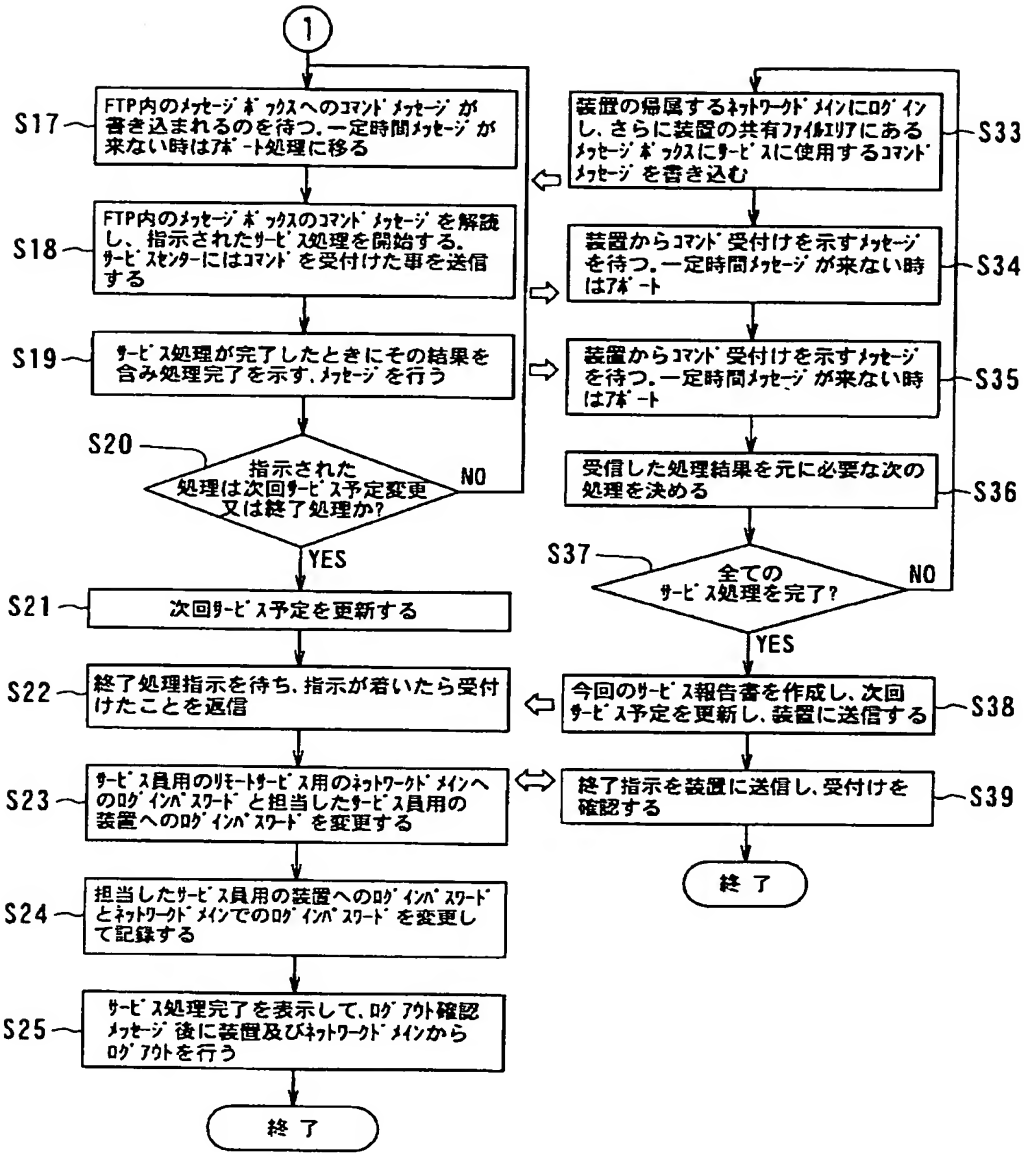
【図４】


据付時処理開始
使用ﾈｯﾄﾜｰｸ環境設定
装置の接続されるDOMAIN名、ﾄﾞﾒｲﾝでのｺﾝﾋﾟｭｰﾀ名、IPｱﾄﾞﾚｽ WINS、DNS、ｹﾞｰﾄｳｪｲ等の設定。
装置の接続されるDOMAINでのｻｰﾋﾞｽ用のﾘﾓｰﾄ用及びｵﾝｻｲﾄ用ﾕｰｻﾞｱｶｳﾝﾄ名・初期ﾊﾟｽﾜｰﾄﾞ
設定(ｻｲﾄのﾈｯﾄﾜｰｸ管理者に作成してもらう。)
ﾌｧｲｱｳｫｰﾙがある場合のその設定
装置ｻｰﾋﾞｽｾﾝﾀｰ間の通信ﾌﾟﾛﾄｺﾙの設定(この例ではFTP)
S1
ｻｰﾋﾞｽｾﾝﾀｰの情報設定
FTPｻｲﾄのIPｱﾄﾞﾚｽ、名前、ｱｶｳﾝﾄ名、ﾊﾟｽﾜｰﾄﾞ
ｻｰﾋﾞｽｾﾝﾀｰのｻｰﾋﾞｽ員の装置へのﾕｰｻﾞｰ名、初期ﾊﾟｽﾜｰﾄﾞの設定
ｵﾝｻｲﾄのｻｰﾋﾞｽ員の装置へのﾕｰｻﾞｰ名、ﾊﾟｽﾜｰﾄﾞの設定
S2
ｻｲﾄからｻｰﾋﾞｽｾﾝﾀｰへの接続試験
ｻｰﾋﾞｽｾﾝﾀｰからの接続への接続試験
ｻｰﾋﾞｽｾﾝﾀｰと装置の相互通信試験
S3
据付時ｻｰﾋﾞｽ(動作確認など)をｵﾝｻｲﾄで実施
初回ｻｰﾋﾞｽ結果をｻｰﾋﾞｽｾﾝﾀｰに通信し記録する。
定期的ｻｰﾋﾞｽｽｹｼﾞｭｰﾙの登録、次回ｻｰﾋﾞｽｽｹｼﾞｭｰﾙの登録
S4
ｻｰﾋﾞｽｾﾝﾀｰへ据付時ｻｰﾋﾞｽ完了を通信
帰属ﾈｯﾄﾜｰｸへの次回ﾛｸﾞｲﾝﾊﾟｽﾜｰﾄﾞの作成とﾄﾞﾒｲﾝｻｰﾊﾞへの登録変更・装置内記録変更
装置への次回ﾛｸﾞｲﾝﾊﾟｽﾜｰﾄﾞの作成と装置内への登録変更・装置内記録変更
S5

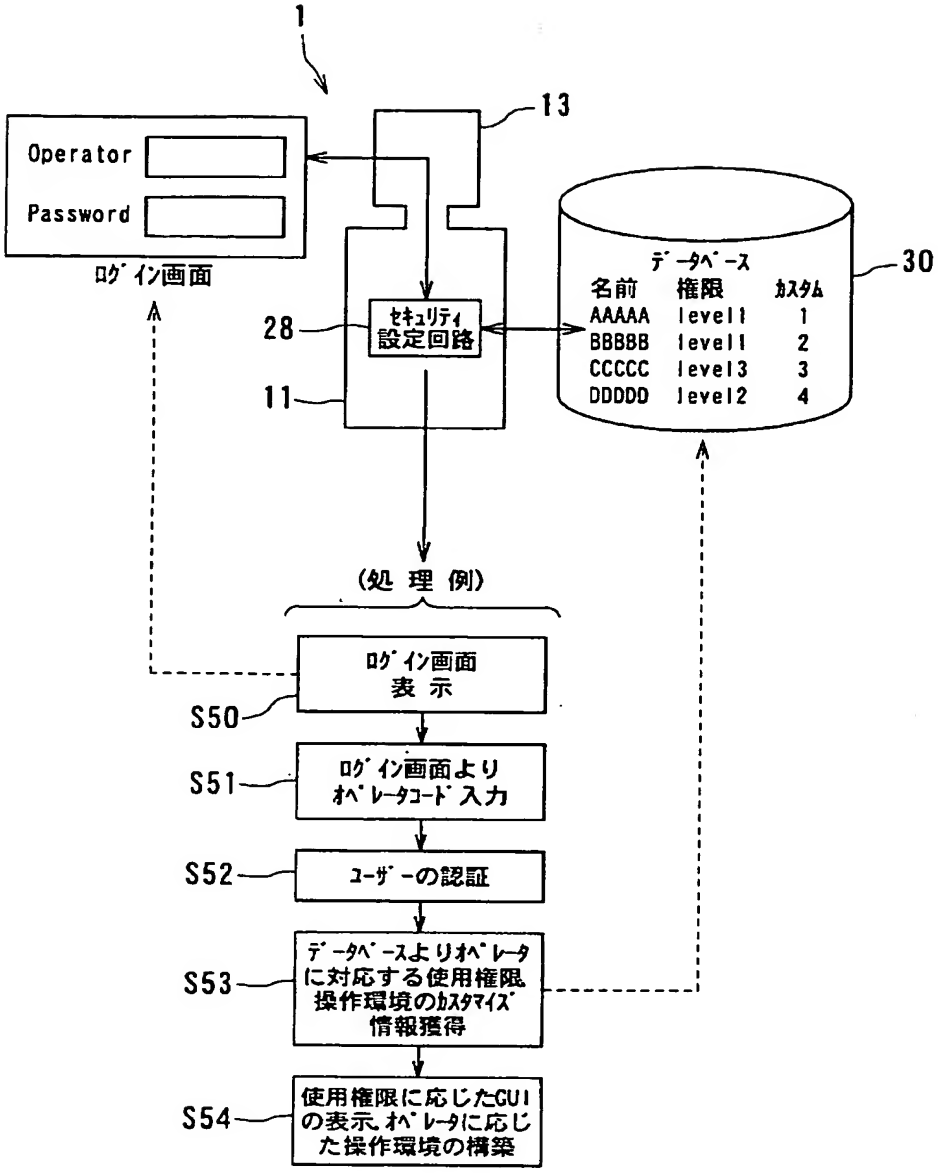
【図５】


装置側の処理
ｻｰﾋﾞｽ要求ｽｲｯﾁ起動
S10
S11
ﾕｰｻﾞが ﾄﾞﾒｲﾝﾕｰｻﾞとして 装置の帰属するﾈｯﾄﾜｰｸに ﾛｸﾞｵﾝしてるか?
S111
ﾕｰｻﾞに対してﾈｯﾄﾜｰｸに接続して ﾛｸﾞｵﾝすることを促すﾒｯｾｰｼﾞを 出すか自動的にﾛｸﾞｵﾝさせる ﾅﾋﾞｹﾞｰｼｮﾝ機能を起動する
S112
S113
ﾕｰｻﾞが ﾛｸﾞｵﾝ処理を中断 していないか?
NO
S114
処理終了
YES
S115
ﾕｰｻﾞが 外部へのﾃﾞｰﾀ 送信の権限を有して いるか?
NO
S116
YES
ﾕｰｻﾞに対して外部へのｱｸｾｽ権限が 無いので電話でｻｰﾋﾞｽｾﾝﾀｰにｺｰﾙする ことを促すﾒｯｾｰｼﾞを出す
S12
ｻｰﾋﾞｽｾﾝﾀｰ内ｻｰﾊﾞへのFTPによるｻｰﾋﾞｽ要求ﾒｯｾｰｼﾞ送信(装置のID、ｻｲﾄのID、ｻｰﾋﾞｽ要求内容を暗号化した情報を含むﾒｯｾｰｼﾞ)
ｻｰﾋﾞｽｾﾝﾀｰ側の処理
ｻｰﾋﾞｽｾﾝﾀｰ内のFTPｻｲﾄ内のﾒｯｾｰｼﾞﾎﾞｯｸｽ内から装置のID、ｻｲﾄのID、ｻｰﾋﾞｽ要求内容を暗号解読し対応するｻｰﾋﾞｽ員を決定し、ｻｰﾋﾞｽ員の情報をFTPのﾒｯｾｰｼﾞﾎﾞｯｸｽに書きこむ
S31
S13
ｻｰﾋﾞｽｾﾝﾀｰ内ｻｰﾊﾞからFTPによりｻｰﾋﾞｽ員の個人名情報取得(ｻｰﾋﾞｽ員のID、名前を暗号化した情報を含むﾒｯｾｰｼﾞ)
S14
ｻｰﾋﾞｽ員の個人名を使用して帰属するﾈｯﾄﾜｰｸでのｻｰﾋﾞｽ員用のﾕｰｻﾞｰｱｶｳﾝﾄとﾛｸﾞｲﾝﾊﾟｽﾜｰﾄﾞと装置へのﾛｸﾞｲﾝﾊﾟｽﾜｰﾄﾞを記録から読み出し、暗号化する
S15
ｻｰﾋﾞｽ員の帰属するﾈｯﾄﾜｰｸﾄﾞﾒｲﾝでのｻｰﾋﾞｽ員用のﾕｰｻﾞｰｱｶｳﾝﾄとﾛｸﾞｲﾝﾊﾟｽﾜｰﾄﾞと装置へのﾛｸﾞｲﾝﾊﾟｽﾜｰﾄﾞの暗号化された第一のﾒｯｾｰｼﾞをFTPを利用してｻｰﾋﾞｽｾﾝﾀｰ内のﾒｯｾｰｼﾞﾎﾞｯｸｽに書きこむ
ｻｰﾋﾞｽｾﾝﾀｰ側の処理
ｻｰﾋﾞｽｾﾝﾀｰ内のFTPｻｲﾄ内のﾒｯｾｰｼﾞﾎﾞｯｸｽ内から装置の帰属するﾈｯﾄﾜｰｸのﾄﾞﾒｲﾝでのｻｰﾋﾞｽ員のﾕｰｻﾞｰｱｶｳﾝﾄとﾛｸﾞｲﾝﾊﾟｽﾜｰﾄﾞ及び装置へのﾛｸﾞｲﾝﾊﾟｽﾜｰﾄﾞを解読する
S32
S16
残りの情報を暗号化した第二のﾒｯｾｰｼﾞをFTPを利用してｻｰﾋﾞｽｾﾝﾀｰ内のﾒｯｾｰｼﾞﾎﾞｯｸｽに書きこむ
①

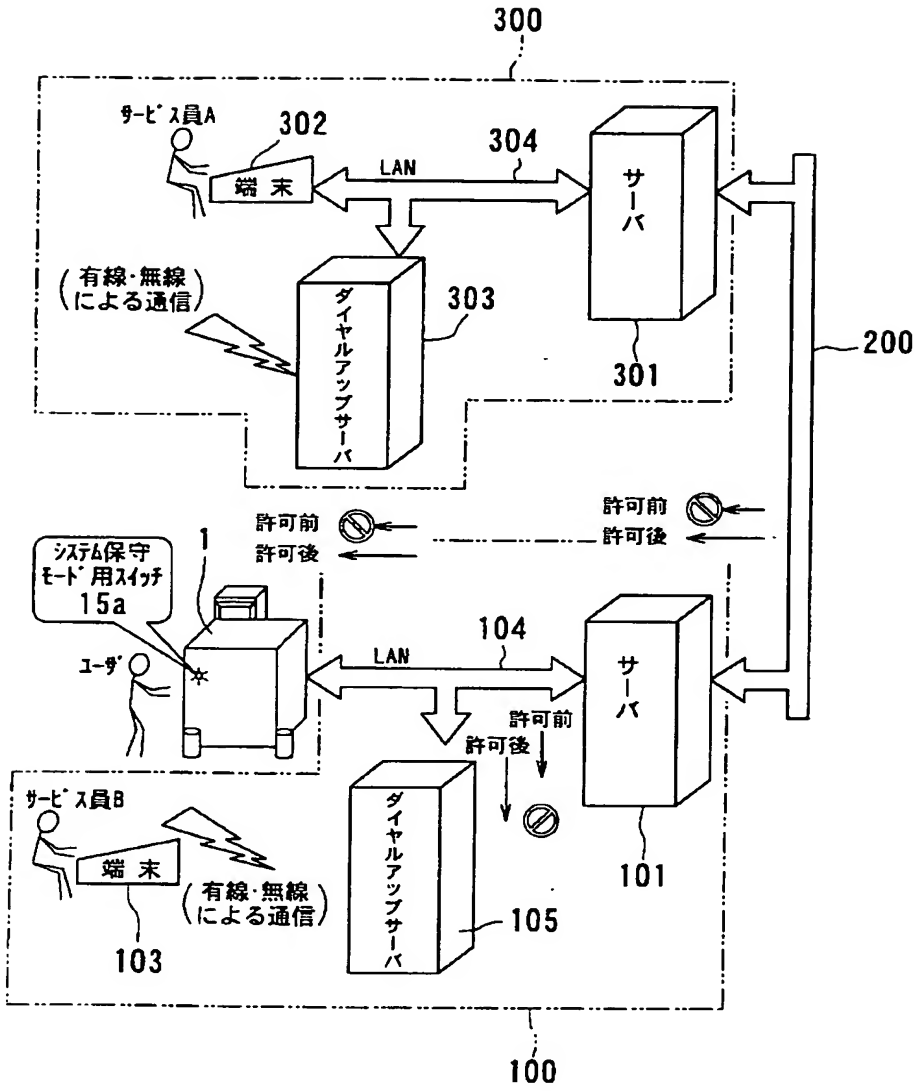
【図６】


①
S17
FTP内のﾒｯｾｰｼﾞﾎﾞｯｸｽへのｺﾏﾝﾄﾞﾒｯｾｰｼﾞが書き込まれるのを待つ。一定時間ﾒｯｾｰｼﾞが来ない時はﾀｲﾑｱｳﾄ処理に移る
S18
FTP内のﾒｯｾｰｼﾞﾎﾞｯｸｽのｺﾏﾝﾄﾞﾒｯｾｰｼﾞを解読し、指示されたｻｰﾋﾞｽ処理を開始する。ｻｰﾋﾞｽｾﾝﾀｰにはｺﾏﾝﾄﾞを受付けた事を送信する
S19
ｻｰﾋﾞｽ処理が完了したときにその結果を含み処理完了を示すﾒｯｾｰｼﾞを行う
S20
指示された処理は次回ｻｰﾋﾞｽ予定変更又は終了処理か?
NO
YES
S21
次回ｻｰﾋﾞｽ予定を更新する
S22
終了処理指示を待ち、指示が着いたら受付けたことを返信
S23
ｻｰﾋﾞｽ員用のﾘﾓｰﾄｻｰﾋﾞｽ用のﾈｯﾄﾜｰｸﾄﾞﾒｲﾝへのﾛｸﾞｲﾝﾊﾟｽﾜｰﾄﾞと担当したｻｰﾋﾞｽ員用の装置へのﾛｸﾞｲﾝﾊﾟｽﾜｰﾄﾞを変更する
S24
担当したｻｰﾋﾞｽ員用の装置へのﾛｸﾞｲﾝﾊﾟｽﾜｰﾄﾞとﾈｯﾄﾜｰｸﾄﾞﾒｲﾝでのﾛｸﾞｲﾝﾊﾟｽﾜｰﾄﾞを変更して記録する
S25
ｻｰﾋﾞｽ処理完了を表示して、ﾛｸﾞｱｳﾄ確認ﾒｯｾｰｼﾞ後に装置及びﾈｯﾄﾜｰｸﾄﾞﾒｲﾝからﾛｸﾞｱｳﾄを行う
終了
S33
装置の帰属するﾈｯﾄﾜｰｸﾄﾞﾒｲﾝにﾛｸﾞｲﾝし、さらに装置の共有ﾌｧｲﾙｴﾘｱにあるﾒｯｾｰｼﾞﾎﾞｯｸｽにｻｰﾋﾞｽに使用するｺﾏﾝﾄﾞﾒｯｾｰｼﾞを書き込む
S34
装置からｺﾏﾝﾄﾞ受付けを示すﾒｯｾｰｼﾞを待つ。一定時間ﾒｯｾｰｼﾞが来ない時はﾀｲﾑｱｳﾄ
S35
装置からｺﾏﾝﾄﾞ受付けを示すﾒｯｾｰｼﾞを待つ。一定時間ﾒｯｾｰｼﾞが来ない時はﾀｲﾑｱｳﾄ
S36
受信した処理結果を元に必要な次の処理を決める
S37
全てのｻｰﾋﾞｽ処理を完了?
NO
YES
S38
今回のｻｰﾋﾞｽ報告書を作成し、次回ｻｰﾋﾞｽ予定を更新し、装置に送信する
S39
終了指示を装置に送信し、受付けを確認する
終了

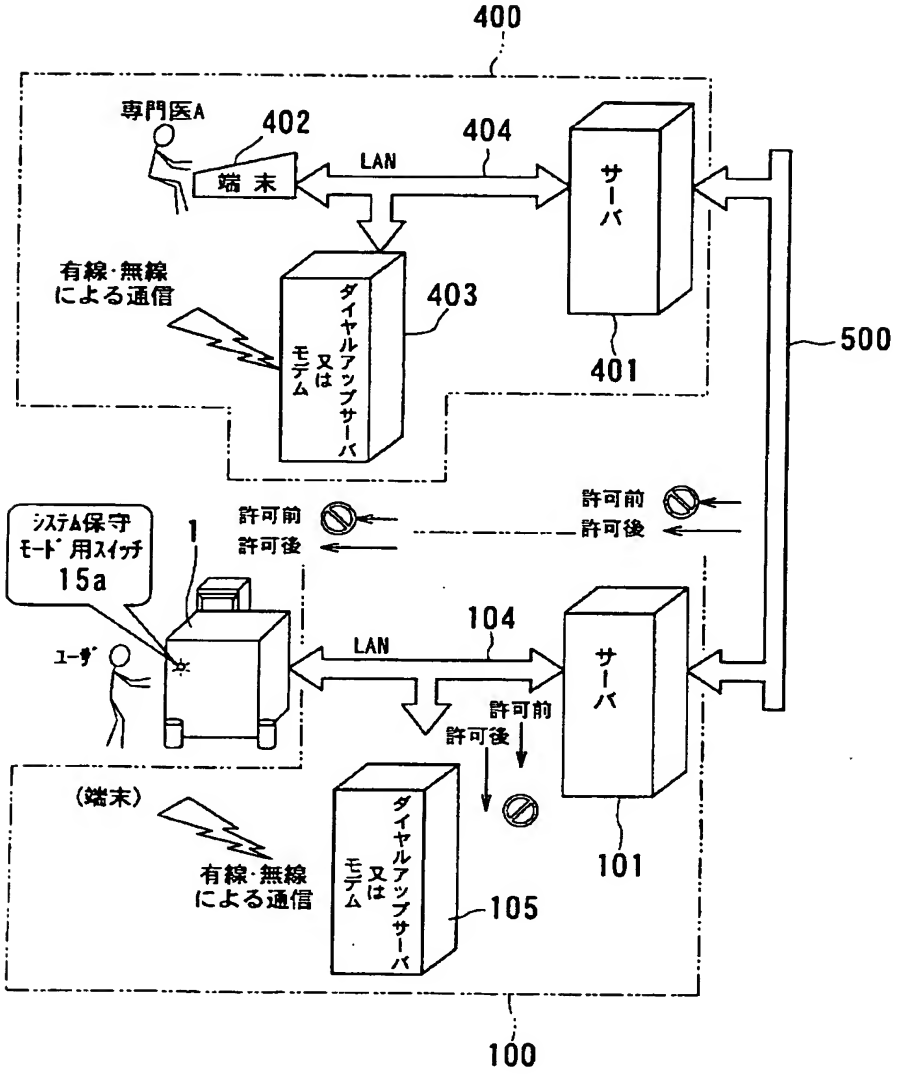
【図７】


1
13
Operator
Password
ﾛｸﾞｲﾝ画面
28
ｾｷｭﾘﾃｨ
設定回路
11
ﾃﾞｰﾀﾍﾞｰｽ
名前 権限 ｶｽﾀﾑ
AAAAA level1 1
BBBBB level1 2
CCCCC level3 3
DDDDD level2 4
30
(処 理 例)
ﾛｸﾞｲﾝ画面
表 示
S50
ﾛｸﾞｲﾝ画面より
ｵﾍﾟﾚｰﾀｺｰﾄﾞ入力
S51
ﾕｰｻﾞｰの認証
S52
ﾃﾞｰﾀﾍﾞｰｽよりｵﾍﾟﾚｰﾀ
に対応する使用権限,
操作環境のｶｽﾀﾏｲｽﾞ
情報獲得
S53
使用権限に応じたGUI
の表示,ｵﾍﾟﾚｰﾀに応じ
た操作環境の構築
S54

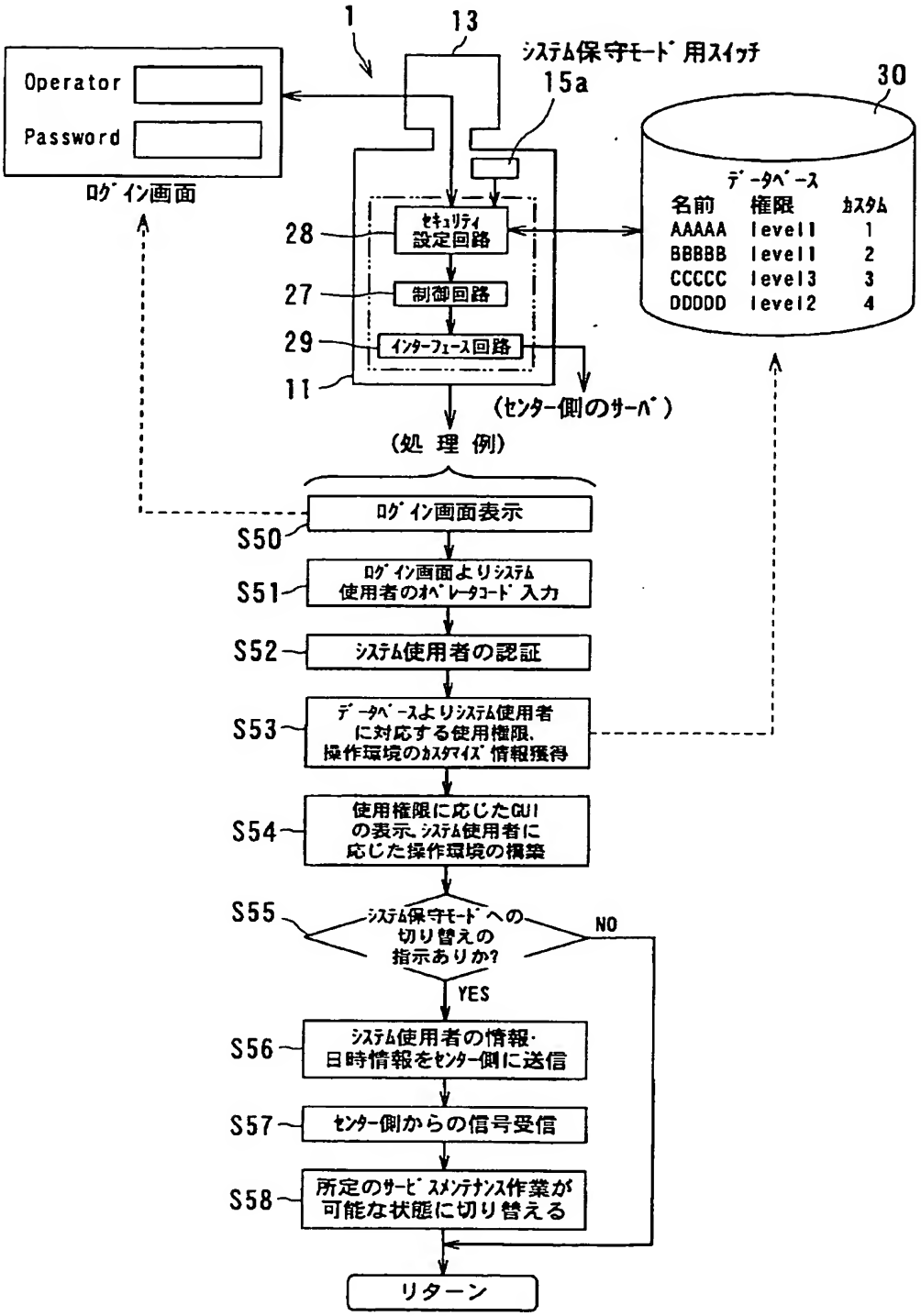
【図８】


300
ｻｰﾋﾞｽ員A
302
端 末
LAN
304
サーバ
(有線・無線)による通信
ダイヤルアップサーバ
303
301
200
許可前
許可後
許可前
許可後
システム保守モード用スイッチ
15a
1
ユーザ
104
LAN
サーバ
許可前
許可後
ｻｰﾋﾞｽ員B
端 末
(有線・無線)による通信
103
ダイヤルアップサーバ
105
101
100

【図９】


400
専門医A
402
端 末
LAN
404
サーバ
有線・無線
による通信
ダイヤルアップサーバ
又は
モデム
403
401
500
許可前
許可後
許可前
許可後
システム保守
モード 用スイッチ
15a
1
ユーザ
104
LAN
サーバ
許可前
許可後
(端末)
有線・無線
による通信
ダイヤルアップサーバ
又は
モデム
105
101
100

【図１０】


1
13
システム保守モード用スイッチ
15a
30
Operator
Password
ログイン画面
データベース
名前 権限 カスタム
AAAAA level1 1
BBBBB level1 2
CCCCC level3 3
DDDDD level2 4
28
セキュリティ設定回路
27
制御回路
29
インターフェース回路
11
(センター側のサーバ)
(処 理 例)
ログイン画面表示
S50
ログイン画面よりシステム使用者のオペレータコード入力
S51
システム使用者の認証
S52
データベースよりシステム使用者に対応する使用権限、操作環境のカスタマイズ情報獲得
S53
使用権限に応じたGUIの表示、システム使用者に応じた操作環境の構築
S54
システム保守モードへの切り替えの指示ありか?
S55
NO
YES
システム使用者の情報・日時情報をセンター側に送信
S56
センター側からの信号受信
S57
所定のサービスメンテナンス作業が可能な状態に切り替える
S58
リターン

フロントページの続き

(72)発明者 橋本 新一
栃木県大田原市下石上字東山1385番の１
株式会社東芝那須工場内
(72)発明者 神山 直久
栃木県大田原市下石上字東山1385番の１
株式会社東芝那須工場内
(72)発明者 吉江 剛
栃木県大田原市下石上字東山1385番の１
株式会社東芝那須工場内
(72)発明者 後藤 英二
栃木県大田原市下石上字東山1385番の１
株式会社東芝那須工場内
(72)発明者 中里 俊章
栃木県大田原市下石上字東山1385番の１
株式会社東芝那須工場内